景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	1/14		生效日期	2012/2/20
文件編號				

壹. 目的

為確保公司資訊系統建置與使用能獲得安全保護，特訂定本辦法。

貳. 權責

一、資訊人員（通報窗口）

1. 資訊系統與網路系統建置、維護與管理
2. 負責接受資訊安全事件通報
3. 資訊安全事件之紀錄
4. 資訊安全事件處理結束後回報通報者

二、資訊主管

1. 督導資訊系統建置與維護
2. 資訊系統變更管制之審核與核准
3. 相關文件之制訂、修訂與廢止、審查
4. 協助委外工作規劃、監控與驗收
5. 資訊安全政策的擬定
6. 負責資訊安全事件之處理、協調、通報、監督、預防及偵測

三、使用單位

1. 資訊使用單位，於資訊委外時須提出委外規劃與需求
2. 遵守安全使用規定

四、人事主管

1. 負責企業員工任用前人員安全背景調查
2. 負責企業內員工安全教育訓練與認知訓練之安排與執行
3. 保密協定的簽訂與保管

五、執行長

1. 企業內文件制訂、修訂與廢止之核准。
2. 各項安全政策的審查與核准

參. 用詞說明

一、事件分類

1. 重大事件：凡所發生之資安事件可能或已造成作業流程、資訊處理設施服務中斷或無法繼續營運時稱之，如電力、電信通訊、辦公場所、網路設備、主機系統受損，或各單位之重要人員或支援機制發生重大變故、人員感染或疑似感染法定傳染病等。
2. 一般事件：凡非屬上述 1. 所述重大事件之資安事件稱之。
3. 外部事件：發生於公司外部的資訊安全事件但足以作為內部參考之事件稱之。

二、事件等級

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	2/14		生效日期	2012/2/20
文件編號				

1. 紅色警訊：當事件發生公司遭受立即財物損失，或事件已造成系統或網路之停頓影響範圍達全公司一半以上使用者且超出 2 小時仍未恢復時，事件將被定義成紅色警訊。
2. 黃色警訊：系統或網路之可用率影響範圍達全公司一半以上使用者且超出 1 小時仍未恢復時，該事件將被定義成黃色警訊。
3. 綠色警訊：其他的事件將被定義成綠色警訊。

肆. 作業內容

一、資訊系統維護/變更管制程序

1. 公司內部資訊系統，包括應用系統、作業系統、網路系統、安全政策等，若須異動時（包括新增、異動、刪除…等），申請人須先填寫〈附表一〉「程式開發/修改申請單」，說明異動原因、問題或需求描述、變更影響範圍、變更類別等送請資訊主管審查。
2. 申請單經資訊主管核准後，交資訊人員依核准意見或方法執行系統變更維護動作。
3. 系統若有相關的文件如系統文件、參考文件或作業準則時，資訊人員於系統變更程序的同時，應同步修改維護相關文件。
4. 若係一般輸入資料更正、軟體設定及硬體維修等則填寫〈附表二〉「資訊設備維修需求單」。

二、資訊安全事件通報程序

1. 公司內同仁若於公司內部發現資訊安全事件發生或外部發生資訊安全事件初步研判可作為內部參考或將會影響公司內部時，應立即通報給資訊人員（通報窗口）。
2. 資訊人員接受通報後應立即知會資訊主管及將事件紀錄於〈附表三〉「資安事件紀錄表」中，並在事件處理結束後知會通報者。
3. 資訊主管可因事件屬性召集相關人員加入事件分析，以協助了解資訊安全技術上的問題，以便共同判定事件屬重大事件或一般事件及其等級。
4. 資訊安全事件經判定分類及等級後，隨即展開通報與處理之程序。若判定為「紅色警訊」時，應即刻通知副執行長（含）以上主管。
5. 資訊安全事件處理過程中，負責人員應將處理情形向主管進行回報。

三、資訊委外管制程序

1. 經內部確認需委外開發後，依據《電腦作業循環》CE-02 系統開發及程式修改作業之規定進行。
2. 委外合約簽定時，應考量委外作業之安全及資訊之重要等級，於合約中訂定

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	3/14		生效日期	2012/2/20
文件編號				

相關的安全與保密條款。若有必要時，可考慮對委外廠商的員工，另簽定個人的保密協定（Non-Disclosure Agreement, NDA），以強化合約的保護能力。相關保密條款及保密協定請參考〈附表四〉之「保密條款範例」及〈附表五〉之「保密協定（NDA）範例」。

3. 委外廠商人員如有派駐公司之情況，資訊系統管理人員需針對該委外人員之電腦系統使用權限予以適當管控。
4. 資訊單位應確實監控開發各階段的完成事項、交付項目及文件等，並確實執行軟體測試項目，將內容及進度填寫於〈附表六〉「程式開發/修改記錄單」。
5. 於委外案結案驗收前，使用單位務必確切使用委外及測試廠商交付的項目，以確保委外交付項目符合當初需求與功能。驗收完成應在〈附表一〉「程式開發/修改申請單」簽核驗收。

四、網路安全作業程序

1. 網路資源管理

- 1.1 資訊人員須於網路系統建置完成時，需將網路連線架構文件化，並依文件管制程序統一管控。
- 1.2 網路連線架構修改時，資訊系統管理人員須依〈一、資訊系統變更管制程序〉進行變更作業。修改後須依文件管制程序同步修改網路連線架構文件。
- 1.3 資訊人員應關閉網路設備或伺服器非必要使用的服務與功能，以降低遭受入侵的風險。
- 1.4 資訊人員於發現網路連線故障或失效時，應立即處理並通知資訊主管。
- 1.5 公司宜建置網路監測系統，資訊人員宜定期提供網路監控報告，呈資訊主管及部門最高主管核閱後存查。

2. 網路安全管理

- 2.1 公司須設置適當防火牆以管制及防範不同網路區之存取需要。
- 2.2 資訊人員依環境或業務需要，於防火牆設定適當規則；防火牆之規則設定政策，依最小需求原則，以正面表列管制並經資訊主管核准後實施。
- 2.3 資訊人員應每周就防火牆進出紀錄進行檢視，如發現可疑之資安事件，須依〈二、資訊安全事件處理程序〉，進行資安事件處理；防火牆進出紀錄至少應保存一個月。
- 2.4 防火牆設定與管理，需加以文件化及說明。
- 2.5 防火牆設定之新增或變更時，資訊人員應依〈一、資訊系統變更管制程序〉進行變更作業，如為防火牆進出規則變更，則須附上〈附表七〉「防火牆規則變更說明表」。
- 2.6 設備或系統廠商如須以遠端（撥接）登入方式進行系統維修時，須先請

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	4/14		生效日期	2012/2/20
文件編號				

廠商以正式之管道通知資訊人員，並經資訊主管同意後才啟動該連線。連線過程中採取適當管制或監控措施，並於系統維修完畢後立即中斷連線。

- 2.7 公司宜設置下列網路防駭機制：弱點掃描、入侵偵測及防禦系統等，以減低或避免資訊系統遭受入侵破壞的可能性，防駭機制運作所產生的紀錄或報表，資訊人員應即時加以檢視，如發現可疑之資安事件，須依〈二、資訊安全事件處理程序〉，進行資安事件處理。
- 2.8 公司應每年委由外界專家或自行評估網路系統的安全性，並依評估結果進行系統修補或系統變更，以提高安全防禦能力。如須變更系統，系統管理人員應依〈一、資訊系統變更管制程序〉進行變更作業。
- 2.9 針對公司開放外界連線之資訊系統，按照資料及系統的重要性，採取資訊加密、身分鑑別、電子簽章等不同安全措施，降低資訊系統受到入侵、破壞、竄改、刪除及未經授權存取的安全風險。

3. 無線網路安全管理

- 3.1 資訊人員須設定使用無線網卡的移動設備（例如：筆記型電腦及 PDA）與無線基地台（Access Point）的通訊必須經過加密。
- 3.2 資訊人員需在無線基地台上登錄公司內部無線網卡 MAC 位址，並只允許這些無線網卡連上無線基地台，以防止未經授權的移動設備連上公司內部網路。

五、電腦安全作業程序

1. 電腦系統與實體設備保護

- 1.1 電腦系統之存取，須設定帳號/密碼管理機制。電腦系統預設之管理員帳號（如：Administrator、root 帳號）須設定密碼保護。
- 1.2 公司內所使用的各式電腦軟體及版權，需集中並經由專人來管理，並定期盤點版權數量是否足夠，如版權數量不足需請資訊主管進行採購。
- 1.3 公司所使用的各式電腦須設定開機（BIOS）密碼。
- 1.4 公司所使用的各式電腦須設定螢幕保護程式並設定密碼，如長時間離開座位或外出應登出或關機。
- 1.5 資訊通訊共用設備，如交換器、防火牆、伺服器等的使用權限須經相關主管核准。
- 1.6 使用任何電腦設備，資訊系統管理人員須注意其電源使用不可超過電源負載量。
- 1.7 資訊通訊共用電腦設備應保存於溫濕度適合的環境並使用不斷電供電系統。
- 1.8 公司可攜式電腦不用時，應存放於上鎖的櫃子或抽屜。

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	5/14		生效日期	2012/2/20
文件編號				

1.9 私人電腦設備嚴禁攜入公司，違者依公司規定送懲。

1.10 廠商維護資訊設備時，應有資訊人員全程陪同。

1.11 對公司所使用的各式電腦（含伺服器、個人電腦、筆記型電腦）均須安裝防毒軟體，並設定自動更新病毒碼機制，且週期性進行完整病毒掃描。

1.12 資訊通訊共用設備須置於具有隔離保護、適當空調及備用電源供應的場所（機房），並登記人員進出的記錄。

1.13 禁止分享 mp3 等多媒體格式檔案及收聽網路收音機，避免大量佔用公司網路資源影響網路頻寬。

2. 密碼安全管理

2.1 所有通行帳號應設定獨立密碼；密碼之設定避免使用容易猜測的字串（例如生日、地名，或密碼與通行帳號相同）。

2.2 密碼存檔或顯示時不可以明文出現。

2.3 在通行帳號第一次啟用時，強制使用者更新密碼。

2.4 原則上資訊人員須設定每三個月更新密碼，最長不得超過六個月否則停用該帳號之機制。

2.5 系統管理者須設定使用者密碼輸入錯誤三次後，系統自動將該帳號暫時鎖定。

2.6 密碼長度應設定至少 6 個字元。

六、應用系統安全作業程序

1. 電子郵件使用安全

1.1 電子郵件系統管理者應依公司內員工之工作性質與業務需要，對電子郵件內容大小進行限制設定。

1.2 資訊人員宜安裝郵件過濾及防毒機制，以過濾垃圾郵件及可能含有病毒之郵件。

1.3 對來路不明的電子郵件，應交由資訊人員處理，不宜隨意打開電子郵件，以免啟動惡意執行檔，使網路系統遭到破壞。

1.4 電子郵件附加之檔案，應事前檢視內容有無錯誤後方可傳送。

1.5 善用公司電子郵件資源，如查獲傳送色情圖片、非法軟體等，依公司規定處理。

1.6 電子郵件附加之檔案應事前檢視檔案之容量大小，如檔案體積超過 10MB 請勿利用電子郵件傳送，更嚴禁將夾帶有大附加檔案之郵件傳送至大型分送清單（如景岳全體員工、光惠全體員工等），只針對必要之人員發送，避免造成郵件風暴嚴重影響網路資源。

2. 資料安全與備份

2.1 資訊主管於規劃資訊架構時應將應用系統資料存放於專屬設備或儲存媒

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	6/14		生效日期	2012/2/20
文件編號				

體，並加以管理。

- 2.2 應用系統資料須定期備份。
- 2.3 資訊主管須規劃定期執行備份資料回復測試，以確保資料備份之有效性。
- 2.4 任何資料儲存媒體報廢時，資訊人應先製作儲存媒體報廢清單，呈資訊主管核准後報廢。儲存媒體報廢時須徹底將其內資料銷毀或消磁。
- 2.5 備份儲存媒體（如磁帶或光碟）須適當地保存於兩地（不可在同一棟建築物內），並加以適當保護。
- 2.6 應用系統之重要資料若列為機密等級，資訊人員需將資訊加密後進行備份，以降低備份媒體內的機密資料遭盜取及濫用的可能性。

七、營運管理

1. 異常事件處理及災害復原計劃

- 1.1 資訊人員須針對常見的資安事件與異常狀況，擬定異常事件處理程序，以增加處理時效，並減低異常事件發生之傷害。
- 1.2 公司須依企業持續經營原則，釐清重大業務衝擊威脅事件，擬定災害復原計劃。
- 1.3 異常事件處理程序與災害復原計畫宜每年至少演練一次並不斷修正，以確保其有效性。

八、人員安全作業程序

1. 人員安全管理

- 1.1 所有員工應簽訂保密合約，不可對外洩漏公司機密。
- 1.2 與安全工作有相關人員離職或轉調工作時，負責該項業務之主管須有適當之安排處理程序，以防止不必要之安全缺失。
- 1.3 對於執行資通安全相關工作或處理機密資訊之員工，人事主管應於任用前進行個人安全背景調查。

2. 安全認知訓練

- 2.1 公司內外若發生重大資訊安全事件（例如最新病毒），經資訊主管核准後應公告予公司員工，以提高員工安全意識。
- 2.2 人事主管應安排及提供定期之資訊安全教育訓練，提高全體員工之資訊安全意識。
- 2.3 人事主管應明文規定員工違反各項資通訊安全時，相關的懲處辦法，以強化員工資訊安全責任感。
- 2.4 公司宜將安全要求納入一般之員工手冊中；亦需加強資訊人員之培訓，以提升資訊安全管理能力。

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	7/14		生效日期	2012/2/20
文件編號				

九、法令遵循

1. 資訊主管應鑑別出公司所需遵循的法規及合約要求，並確實遵守。
2. 資訊主管應調查並瞭解公司套裝軟體使用情形，並採購足夠的版權。
3. 資訊主管應確保公司對外網站不得公佈機密性、敏感性及未經當事人同意之個人隱私資料。

伍. 本辦法經執行長核准後公布實施，修正時亦同。

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	8/14		生效日期	2012/2/20
文件編號				

<附表一> 程式開發/修改申請單

景岳生物科技股份有限公司 程式開發/修改申請單

編號：(MIS 依年度編製流水號)

申請人		申請單位		申請日期		需求日期	
模組				程式/ 報表名稱			
需求說明							
效益說明							
使用頻率				節省工時			
使用者				使用限制			
資訊部門 主管			資訊人員			申請單位 主管	
相關單位 會簽意見							
驗收記錄							
資訊單位 主管			申請單位 主管			申請人	

※系統程式開發/修改申請流程如下：

1. 使用單位填寫本申請單→申請部門主管核准→資訊單位受理
2. 外包廠商評估並開立規格→申請人確認規格→會簽相關單位（指該程式修改所影響之單位）
3. MIS 記錄開發過程於「程式開發/修改記錄單」→包商開發完成→MIS 通知使用單位驗收、測試
4. 系統核定啟用結案

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	9/14		生效日期	2012/2/20
文件編號				

〈附表二〉 資訊設備維修需求單

景岳生物科技股份有限公司

資訊設備維修需求單

表單編號：

單位：	需求者：
申請日期：	需求日期：
聯絡電話：	
☐ 硬體維修 ☐ 軟體設定 ☐ 系統輸入資料之更正 ☐ 其他_____	
需求描述：	

部門主管：

需求者：

處 理 回 報
☐ 非法軟體清查：

(本欄資訊單位填寫)

資訊單位主管：

部門主管：

需求者確認：

處理者：

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	10/14		生效日期	2012/2/20
文件編號				

<附表三> 資安事件紀錄表

景岳生物科技股份有限公司

資安事件記錄表

事件編號		接案日期		結案日期	
事件簡述					
事件分類	☐ 重大事件； ☐ 一般事件； ☐ 外部事件		等級	☐ 紅色 ☐ 黃色 ☐ 綠色	
影響範圍					
服務中斷時間				損失金額	
日期	處理軌跡			追蹤註記	

部門主管：

記錄：

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	11/14		生效日期	2012/2/20
文件編號				

<附表四> 保密條款範例

第**條保密條款

- 一、一方執行本合約之過程中，若需使用他方之機密文件時，應依循他方規定之程序申請之。
- 二、本合約之各項資料與文件，雙方不得將其全部或部分借予、給予或售予第三者。
- 三、任一方因本合約獲知他方指明為機密之資訊、物件、設備，未經他方書面同意，不得運用於與本約無關之工作，且應防止遭第三者知悉、獲取。但上述機密之公開，非可歸責於獲知之一方時，例如：機密已由對方或他人公開、或公開因法令之要求，不在此限。
- 四、合約期間，任一方若因可歸責於己之事由有洩露他方指明為機密資料之情事時，並經舉證屬實後，他方得予解約，若因此造成他方之損失（限於直接損失且不包括所失利益）時，他方並得就該損失要求賠償。
- 五、合約期滿後_____年內，雙方亦應依誠信原則保守彼此相關業務機密；保密義務消滅後，接收方應依揭露方要求銷毀或返還機密文件、物品、設備，不留存任何備份。揭露方未於保密義務消滅後*個月內為前述要求，接收方不負保管之責。
- 六、乙方違反本契約本條款之規定時，應支付甲方新台幣_____萬元之懲罰性賠償；如有其他損失，並應另行賠償。

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	13/14		生效日期	2012/2/20
文件編號				

〈附表六〉程式開發/修改記錄單

景岳生物科技股份有限公司 程式開發/修改記錄單

編號：(依程式開發/修改申請單編號)

程式開發/修改時程		資訊單位記錄			
日期	預計完成事項	日期	實際進度記錄	主管確認	
應交付項目 及文件 <small>(完成時填寫)</small>					
外包廠 商確認		資訊部 門主管		資訊 人員	

※系統程式開發修改記錄單流程如下：

1. 資訊單位接獲申請單位「程式開發/修改申請單」，應將整個程式開發/修改過程記錄於本單上。
2. 填寫預計程式開發/修改時程→實際進度記錄→完成→通知使用單位驗收(於「程式開發/修改申請單」簽名)→應交付之項目及文件→資訊主管及包商雙方確認→系統核定啟用結案

景岳生物科技股份有限公司

制定部門	稽核	資通安全作業辦法	制定日期	2012/2/20
版本	1.0		適用部門	所有部門
頁次	14/14		生效日期	2012/2/20
文件編號				

<附表七> 防火牆規則變更說明表 (範例)

景岳生物科技股份有限公司

防火牆規則變更說明表

事由	
變更影響說明	
變更項目	☐ 新增 ☐ 修改 ☐ 刪除
規則： 來源 IP 位置： 目的 IP 位置： 使用之通訊埠： 規則有效期間： 其他說明：	

部門主管：

申請人：