資訊安全政策	初　版　日	2010.11.01	文件編號	CCIS-1-001
	生　效　日	2019.03.20	版　　本	9
	制定單位	制度小組	頁　　次	1/7

第一條 目的：

為確保本公司之資訊安全管理系統得以有效運作與執行，使資訊安全政策、資訊安全目標與資訊安全各流程清楚展現與說明。

第二條 範圍：

資訊安全管理系統所涵蓋之所有流程與單位均適用，從電腦機房之資料管理、網路資源服務、提供資訊系統開發...等均依循 ISO 27001:2013 年版之資訊安全管理系統之標準要求。

第三條 權責：

一、資訊安全政策核准：本公司資訊安全組織主任委員 總經理。
二、資訊安全政策修訂審核：由資訊安全組織制度小組提出，經由主任委員核准修訂之。
三、資訊安全政策制訂與修改： 由資訊安全組織制度小組制訂。
四、資訊安全政策作廢：由資訊安全組織制度小組制訂提出，經主任委員核准作廢。

第四條 名詞解釋：

資訊安全：所謂資訊指的是本公司在營運時所收集、產生或運用的資料，它可以存在於任何形式，不論是有形或無形的，它可以是存在於電腦中的資料，列印或書寫在紙張上的資訊，甚至是存在於通訊中；這些資訊都是屬於本公司的資產。資訊安全即為了避免因人為疏失、蓄意或自然災害等風險，運用適當的控制措施，包括政策、實踐、步驟、組織結構和軟體功能等，來確保公司的資訊資產受到妥善的保護。

第五條 作業內容

一、本公司簡介

(一)公司名稱：中華徵信所企業股份有限公司
(二)公司地址：台北市信義區東興路 59 號 5 樓
(三)連絡電話：+886-2-8768-3266
(四)傳真號碼：+886-2-8768-2033
(五)員工人數：90 人
(六)公司沿革：

中華徵信所自 1961 年成立以來，以工商徵信為根本，由中心輻射至周邊，逐漸枝繁葉茂，衍生了各種工商資訊服務，為國內最大的專業徵信公司，亦是國內少數提供全方位工商資訊服務且信譽卓著的企業集團，扮演著協助政府及工商企業的角色掌握了台灣經濟的脈動，深刻留下歷史見證的軌跡。

其餘詳細資料請參考本公司網站簡介 -- 中華徵信所企業網站

（七)地理位置

二、組織背景：

（一） 本公司資訊安全組織應決定與資訊安全管理相關內外部問題(法規、公司政策、客戶或主管機關求)及利害相關團體(員工、供應商、股東)需求與期望。

（二） 每年於管理審查會議時提出相關議題的研討，並完成『組織全景及策略規劃表』，以作為資訊安全管理系統範圍適用性的確認及風險評估之依據。

（三） 資訊安全組織應決定及規劃資訊安全管理系統有關的內部與外部溝通的需求，並將規劃結果登錄於『ISMS 溝通規劃表』。

三、資訊安全政策：

（一)中華徵信所企業股份有限公司資訊部門(以下簡稱本部門)為強化資訊安全管理、增進同仁對資訊安全之認知，並確保資料、系統、設備與網路安全，特訂定本政策。

（二） 為統籌資訊安全管理等事項之協調及推動，成立本公司資訊安全組織，並要求公

司各部門都派員參加資訊安全項目之計劃與推動，有關資訊安全組織架構與各工作小組權責，請詳見本小節後續定義說明。

（三）本公司制訂資訊安全政策的目標，在於提高資訊系統的可靠性，加強資訊系統的可用性，以保護公司資訊資產；並建立安全的使用操作程序，提升客戶對本公司的信用度。

（四）為推動本公司資訊安全計畫，特訂定本公司的資訊安全政策的計畫目標：

資安教育要確實 資安防護要做好 風險管理要有效

（五）為達成本公司資訊安全政策的目標，資訊安全的工作規範至少須符合『資訊安全目標規劃表』中所列項目的要求，並於規畫表中明列執行方式與資源需求之欄位，以做完整之目標規劃。

（六）高階管理者應展現領導能力，以及與資訊安全管理系統有關的承諾，以確保下列事項：

- 確保資訊安全政策與目標已建立，並且與組織的策略方向一致。
- 確保資訊安全管理系統的要求已融入組織過程中，及所需的資源可取得。
- 溝通符合資訊安全管理的重要性，並且遵守資訊安全管理系統的要求。
- 確保資訊安全管理系統達成預期結果。
- 指導與提供支援，讓人員對資訊安全管理系統有效性做出貢獻，並促進持續改進。
- 支援其他的相關管理角色，展現出在職責運用上的領導能力。

（七）本政策之範圍如下，有關單位及人員應就下列事項訂定相關管理規範或實施計畫，並定期評估實施成效：

一、資訊安全本組織人員管理及資訊安全教育訓練。
二、電腦系統安全管理。
三、網路安全管理。
四、系統存取控制。
五、系統發展及維護安全管理。
六、資訊資產安全管理。
七、實體及環境安全管理。
八、行動媒介管理。
九、備份資料、電子商務等伺服器日常監控管理。

十、日常作業與帳號密碼管理。
十一、 資訊安全事故/事件管理。
十二、 業務永續運作計畫之規劃與管理。
十三、 資訊安全政策之適用性。

（八）人員管理及資訊安全教育訓練

- 對資訊相關職務及工作，應進行安全評估，並於人員晉用、工作及任務指派時，審慎評估人員之適任性，並進行必要的考核。
- 針對管理、業務及資訊等不同工作類別之需求，定期辦理資訊安全教育訓練及宣導，建立同仁資訊安全認知，提升資訊安全水準。

（九）電腦系統安全管理

- 辦理資訊業務委外作業，應於事前研提資訊安全需求，明訂廠商之資訊安全責任及保密規定，並列入契約要求廠商遵守並定期考核。
- 依相關法規或契約規定複製及使用軟體，並建立軟體使用管理制度。
- 採行必要的事前預防及保護措施，偵測及防制電腦病毒及其他惡意軟體，確保系統正常運作。

（十）網路安全管理

- 開放外界連線作業之資訊系統，應視資料及系統之重要性及價值，採用不同安全等級之技術或措施，防止資料及系統被侵入、破壞、竄改、刪除及未經授權之存取。
- 與外界網路連接之網點，應控管外界與內部網路之資料傳輸與資源存取。
- 利用網際網路及全球資訊網公布及流通資訊，應實施資料安全監控，具有機密性、敏感性或未經當事人同意之個人隱私資料及文件，不得公布。
- 須訂定電子傳輸使用規定，機密性資料及文件不得以電子郵件或其他電子方式傳送。

（十一）系統存取控制

- 系統存取應依人員職務或角色，訂定相關權限。
- 離(調)職人員，應取消各項資訊資源之所有權限，並列入離(調)職之必要手續。人員職務調整及調動，應依系統存取授權規定，限期調整其權限。
- 建立系統使用者註冊管理制度，加強使用者通行密碼管理，使用者通行密碼之更新周期，須在帳號與密碼管理程序中予以規範。
- 對系統服務廠商以遠端登入方式進行系統維修者，應加強安全控管，課其相關安全保密責任。
- 需建立資訊安全稽核制度，定期或不定期進行資訊安全稽核作業。

（十二）系統發展及維護安全管理

- 自行開發或委外發展系統，應在系統生命週期之初始階段，即將資訊安全需求納入考量
- 系統之維護、更新、上線執行及版本異動作業，應予安全管制，避免不當軟體、暗門及電腦病毒等危害系統安全。
- 對廠商之軟硬體系統建置及維護人員，應規範及限制其可接觸之系統與資料範圍，並嚴禁核發具有長效性之系統辨識碼及通行密碼且使用完畢後應立即取消其使用權。
- 受委託之廠商於建置及維護重要之軟硬體設施時，應在本公司相關人員同意後始得為之；如果在機房維護系統期間，必須有本公司負責人員全程陪同監測廠商之行為。

（十三）資訊資產安全管理

- 建立與資訊系統有關的資訊資產清冊，訂定資訊資產的項目、擁有者及資訊資產分類等。
- 已列入資訊資產安全分類的資訊及系統之輸出資料，應標示適當的安全等級以利使用者識別與遵循。

（十四）實體及環境安全管理：就設備安置、周邊環境及人員進出管制等項目，需訂定實體及環境安全管理措施。

（十五）行動媒介管理：必須建立控管流程，各單位主管與資訊部人員可以開放 USB 行動儲存媒介使用；各單位如有需求可以提出申請依照相關流程辦理。

（十六）備份資料、電子商務等伺服器日常監控管理：依據公司所經營之業務項目，所提供支電子商務與營運相關系統，必須進行日常維護作業，規劃備份作業，保證系統運作正常；相關備份紀錄與監控資料須保存 3 個月以上；電子商務網站應注意資訊的機密性與完整性，避免個資或是其他資訊的不當洩漏。

（十七）日常作業與帳號密碼管理：系統管理員應配發使用者帳號，並規範登入系統的使用權限，防止蓄意或非故意的違法存取系統檔案或公用程式；密碼須定期更新，禁止記錄於媒體使用；並定期檢查與稽核系統相關紀錄，保障相關資料的機密與安全。

（十八）資訊安全事故/事件管理

- 各項資訊安全活動或服務過程之意外與緊急事故鑑定。
- 資訊安全緊急事故通報。
- 資訊安全意外與緊急事故應變之測試。
- 持續監控、管理及改善資訊安全。

（十九）業務永續運作計畫之規劃與管理

- 訂定業務永續運作計畫，評估各種人為及天然災害對業務運作之影響，訂定緊急應變及回復作業程序及相關人員之權責，並定期演練及調整更新計畫。
- 建立資訊安全事件緊急處理機制，在發生資訊安全事件時，應依規定之處理程序，立即向資訊單位或人員通報，採取反應措施，必要時，並聯繫檢警調單位協助偵查。

（二十）本政策應至少每年評估一次，以反映政府法令、技術及業務等最新發展現況，確保資訊安全實務作業之有效性。

（二十一） 本資訊安全管理政策由資訊部門主管核可，並呈報總經理核准後實施，修正時亦同。

第六條 資訊安全政策制(修)訂、廢止、分發及管制規定：

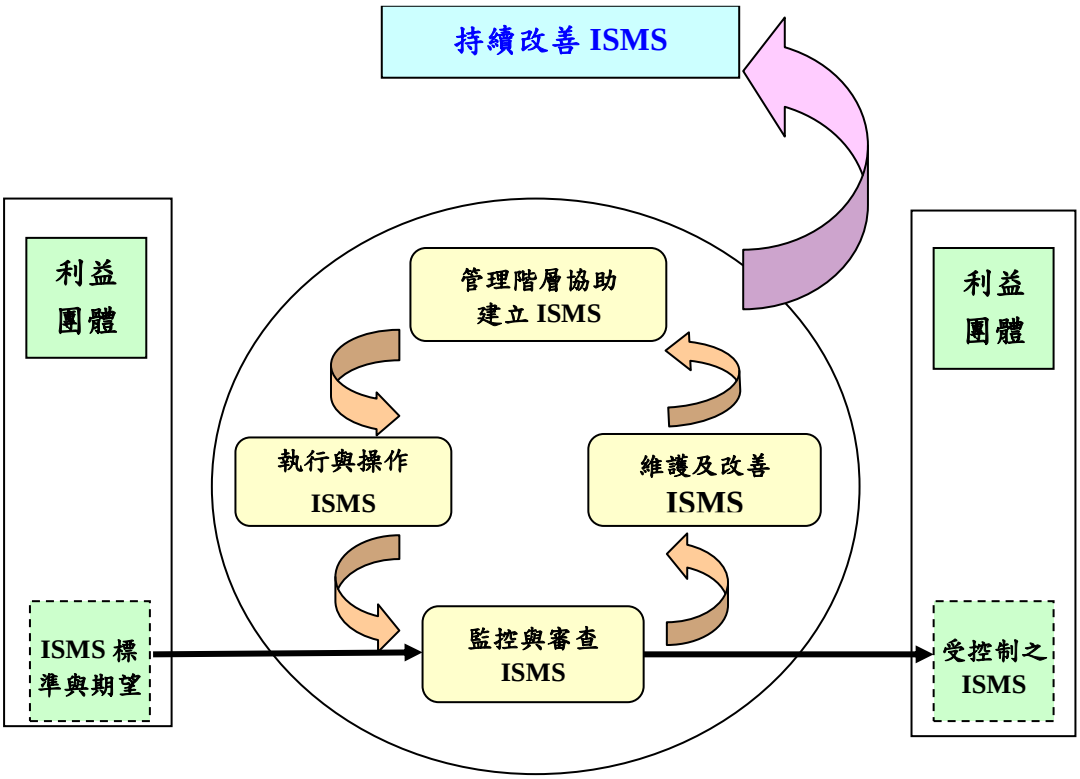
（一） 資訊安全政策之制(修)訂、廢止流程依照「資訊安全文件與紀錄管理程序」規定辦理，政策相關之制度文件制訂後須經由總經理審閱同意，始可正式發行。

（二） 資訊安全政策之分發及管制規定流程依照「資訊安全文件與紀錄管理程序」規定辦理。

- 資訊安全政策採用電子發行，所以文件經核准並同意正式發行後，相關文件管制人員應將電子文件轉成 PDF 檔，上傳到內部網站後，再以 E-mail 通知文件權責相關同仁，自行到內部網站確認文件內容。
- 本手冊不得任意影印，若因服務或宣導資訊安全需求，需由主管核准發送。

第七條 資訊安全系統模式：

資訊安全政策	初　版　日	2010.11.01	文件編號	CCIS-1-001
	生　效　日	2019.03.20	版　　本	9
	制定單位	制度小組	頁　　次	7/7



第八條　公司資訊安全政策適用於公司全體同仁，若有例外管理規定須於各相關管理規範或計畫中另行明確訂定。

第九條　附件：

一、適用性聲明(CCIS-1-001-001-2)

二、組織全景及策略規劃表(CCIS-1-001-002-1)

三、ISMS溝通規劃表(CCIS-1-001-003-1)

編修日期	說明
2010.11.01	新訂
2011.12.10	修訂
2012.12.27	修訂
2014.11.25	修訂
2015.04.15	修訂
2016.12.10	修訂
2017.04.01	修訂
2019.04.01	修訂
2020.03.15	修訂