欣屏天然氣股份有限公司

個人資料保護維護計畫作業要點

壹、依據

一、行政院個人資料保護委員會公告個人資料保護法施行。

二、經濟部個人資料保護作業手冊。

三、經濟部能源署「電業及公用天然氣事業個人資料檔案安全維護管理辦法」。

貳、目的

針對涉及個人資料之蒐集、處理、利用與管理程序，制訂此作業要點。期使各部門在處理員工及用戶個人資料時，能有效善盡管理保護之責任，杜絕人為不當利用致引發個資洩漏之資安事件，確保公司企業形象。

參、適用範圍

有關員工個資、用戶申辦掛表、拆表、過戶、退費業務，本公司所有蒐集屬於「個人資料保護法」規定的個人資料，包含全體員工、委外服務廠商、資料使用者與訪客等，均應確實嚴密保護不得洩漏。

一、紙本資料：員工管理(人事資料袋)、用戶臨櫃申辦案件所提供之身分證影本、房屋所有權狀影本等個人資料(用戶資料袋)。

二、傳真資料：用戶傳真申辦案件所提供之身分證影本、房屋所有權狀影本等個人資料。

三、報表暨表單資料：有關申辦案件所產生之報表及表單資料。

四、電子檔案：儲存於系統資料庫之員工、用戶個人資料檔案。

肆、作業要點

一、設置「資訊安全暨個人資料保護委員會」

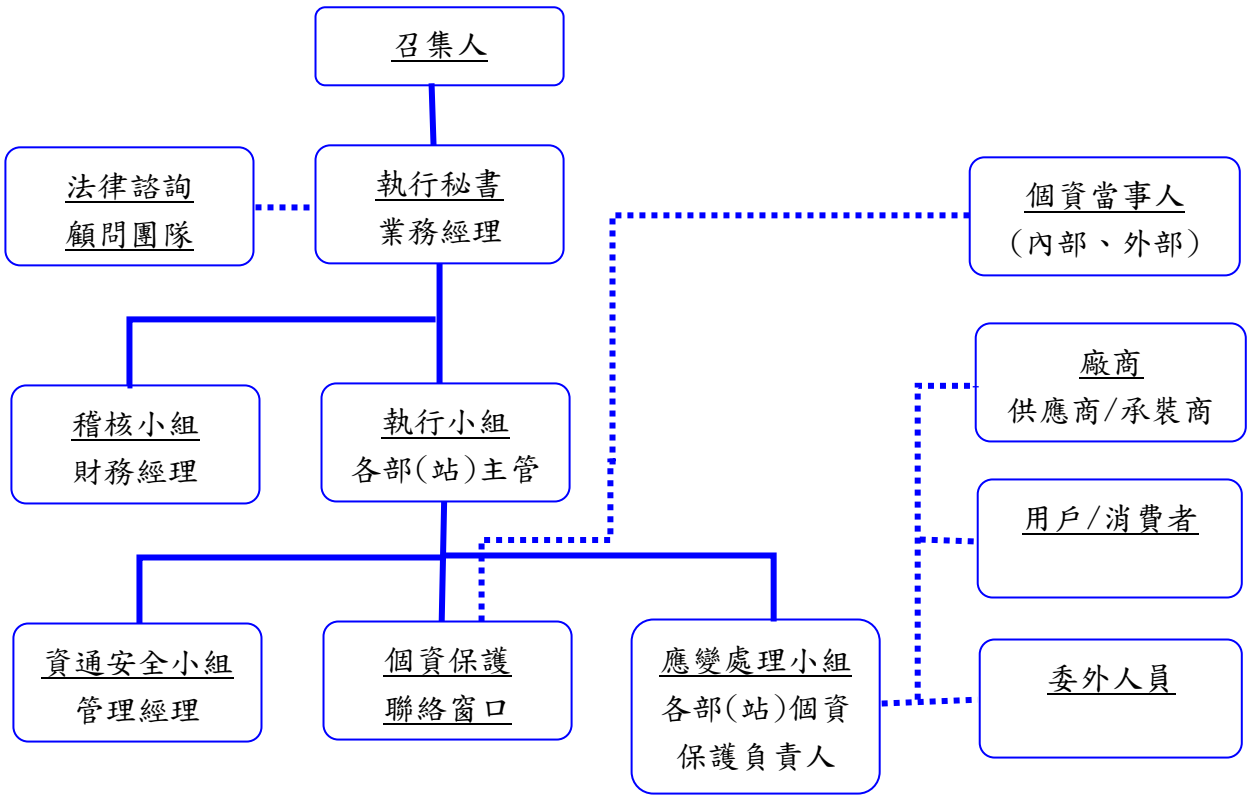
(一)依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 1 款規定辦理，為使本公司資訊安全管理系統及個人資料保護管理系統充分發揮資訊安全暨個人資料保護管理功能，設置「資訊安全暨個人資料保護委

員會」 編組(以下簡稱委員會)，由總經理擔任召集人，資訊組長擔任執行秘書，納編各部(站)主管，個資業管負責人編成執行小組、稽核小組及緊急處理小組暨個資保護聯絡窗口，並委吳澄潔法律事務所擔任本公司法律諮詢顧問團隊。

(二)本委員會之任務如下：

1. 制定本公司資訊安全及個人資料保護政策。
2. 監督與稽核本公司資訊安全及個人資料保護管理機制之運作。
3. 本公司資訊安全及個人資料保護風險之評估與改善。
4. 本公司資訊安全及個人資料保護緊急事件之應變處理。
5. 依風險類別、識別說明及執行情形，納入年度「風險管理運作情形」報告。

欣屏天然氣股份有限公司資訊安全暨個人資料保護委員會



(三)各部(站)應建立：

1.個人資料保護業務之協調聯繫及緊急應變通報。

2.非資通安全面個人資料安全事件之通報。

3.重大個人資料外洩事件之用戶聯繫單一窗口。

4.個資法第 18 條及個資法施行細則第 12 條所定個人資料檔案安全維護。

5.員工之個人資料保護意識提升及教育訓練計畫之執行。

6.個人資料保護事項之協調聯繫。

7.個人資料保護方針及政策之執行、單位內個人資料保護之自行查核。

8.個人資料保護管理之規劃及執行。

二、個資定義：

自然人之姓名、出生年月日、國民身分證統一編號、護照號碼、特徵、指紋、婚姻、家庭、教育、職業、病歷、醫療、基因、性生活、健康檢查、犯罪前科、聯絡方式、財務情況、社會活動及其他得以直接或間接方式識別該個人之資料。

三、個資蒐集作業要點：

蒐集個人資料時，應有特定目的並符合特定情形(個資法第 15 條)。

(一)用戶申辦案件，針對該項所需資料蒐集，如建物權狀影本、房屋稅單、買賣契約書、身分證、駕照、健保卡等證明文件。其他與業務無關事項不得蒐集、拷貝、傳遞、攜出或告知非業務承辦人。

(二)用戶退費案件，需影印之身分證、駕照、健保卡、匯款帳號等證明文件時，應在影印本加蓋「僅限欣屏公司申請案件使用，他用無效」章；如匯入原扣款帳號或原繳款人帳號，則只核對個人資料不需再影印任何個人資料。

(三)影印或傳真資料不良者，一概投入碎紙機內銷毀，避免遭人利用。

四、個資處理作業要點：

處理個人資料時，應有特定目的並符合特定情形(個資法第 15 條)。

(一)未處理完成之案件，下班後不得置於辦公桌，以免遭有心人士利用、

影印、拷貝、傳遞、攜出。

(二)員工個人資料、承商及用戶申辦案件，所提供之資料僅限與該業務相關之事項使用，不得移作他用。

(三)離開辦公桌時應將電腦畫面登出，避免非業務承辦人閱覽。

(四)所有資料存取工作均應使用帳號密碼,並由電腦系統自動辦理存取登錄，以利追蹤查考。

(五)重要或具機密性資料應自行錄製建檔，並建立資料存取控制區分。

五、個資利用作業要點：

以個資法第 15 條第 2 款「經當事人同意」方式蒐集個人資料時，對於個人資料之利用應符合該同意書所載之內容,包括個人資料利用之期間、地區、對象、方式及其他相關事項。

(一)蒐集之資料限用於裝表、抄表、計費、收費、定期檢查、銷售、維修及與本公司瓦斯相關之業務。

(二)各部門電腦操作人員所使用的建檔、查詢與列印程式，需經核可授權才能取得完整個人資料，其餘人員均限縮個資資訊之取得，採不顯示或資訊隱藏方式，以維護資訊安全。

(三)各部門產生列印的各類明細報表或統計報表,由各當事人負責運用與保管。文件含有員工、客戶個資時，依照資訊安全作業規定，不可任意閑置桌上或丟棄;任何廢棄不用之報表都必須集中存放並由專人保管，定期再依規定辦理銷毀。

(四)一般性的報表或查詢功能，全數剔除個資資料。

(五)個資資訊之取得權限,由業管單位專案簽呈或填寫軟體需求單經批示奉准後辦理程式異動，且於人員執行列印或查詢完整個資時，留下電腦存取紀錄，作為日後稽核及企業舉證之用。

(六)確有必要公布個人資料於公司網站時，應遵守相關法律及規範處理，並另需簽奉核准後始得公佈。

(七)禁止使用即時通訊軟體、外部信箱傳輸個人資料檔案。與金融單位交易作業時，傳輸帳務檔案發送個資資訊時必須加密保護。

(八)檢視一般個人資料之利用,是否符合相關規定蒐集之特定目的必要範

圍；為特定目的外之利用者，檢視是否符合法定情形；其經當事人同意者，應符合主管機關相關規定之處理原則。

六、個資保存作業要點：

(一) 掛（拆）表之用戶資料附於服務作業單、退費申請處理單、過戶申請書，由業務部造冊並歸檔。

(二)抄表卡於使用年度到期後，分別依作業代號裝箱留存於六樓儲藏室。

(三) 抄表卡、帳單地址變更及臨櫃繳費收據等於保存期滿時，雇請立案環保廠商派員隨車至公立焚化廠燒毀。

(四)員工個人資料、勞工健檢等，統一由管理部人資存管，另離職員工應保存 5 年後，始可造冊簽核銷毀。

(五)定期檢視個人資料之有效性及可用性，刪除或銷毀不必要之個人資料。

(六)保有個人資料蒐集之特定目的消失、期限屆滿或違法蒐集時，各部門應主動或依當事人之請求刪除或銷毀該個人資料。但特定目的消失或期限屆滿時，因執行職務所必須或經當事人書面同意者，不在此限(個資法第 11 條第 3 項、第 4 項)。

(七)依前目規定刪除或銷毀個人資料時，應由資料蒐集單位簽奉核定後，移由資料保有單位刪除或銷毀。

七、個資管理作業要點：

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 6 款及第 8 款規定辦理，以有效規範個人資料之安全管理作業，防止個人資料發生被竊取、竄改、毀損、滅失或洩漏等事故。

(一) 所有資料存放區平時上鎖管制，分由各部門統一存管，並律定專人管理。

(二) 各部門指定一至二人擔任公文資料調閱員，負責該部門所有用戶資料之調閱及歸還事宜(公文文書檔案調閱仍由相關承辦人負責)，以釐清責任分界。

(三) 借調或調用之檔案應妥慎保管，不得遺失、轉借、轉抄，或有拆散、污損、添註、塗改、更換、抽取、增加、圈點等破壞檔案或變更檔

案內容之情事。

（四）承裝商及會計師等外部人員不得自行調閱資料。

（五）具有個資之廢棄文件以碎紙機處理，不再回收利用。

（六）各部門辦公室內部資料保管及樓層影印機管理，請相關部門指派專人負責。

（七）員工到職應即簽署「資訊安全保密切結書」(格式如附件一)。

(八)相關合作廠商應簽訂「個資保密合約書」(格式如附件二之一及之二)。

伍、電腦資料管理作業規定

一、於存取限閱級之資料時，即同時自動記錄每一帳號對該筆記錄之查詢、新增、更正、註銷等的異動時間及內容，並將記錄保留一年以上，以利查考。歷史記錄可依需要隨時提供檢查之。

二、業務承辦人員要求電腦系統人員修改程式或資料媒體內容時：

（一）若涉及機密性資料或具有影響公司收益的資料與程式時，必須經簽奉核定後辦理，並應將修改內容、時間及作業人員等資料詳實記錄備查。

（二）若不涉及機密資料或程式，惟因該修改與其它單位相關連時，仍需簽奉核定後辦理之。

三、未經授權單位之人員欲查閱限閱級資料時，應簽奉核定後始可查閱。

四、輸出入之報表，在處理前後均應妥加保存，處理過程中應注意保密，如屬機密資料應以密件處理。

五、各單位主管應對所屬作業情形，實施定期與不定期之考核，並加以記錄。

六、各單位電腦作業所需之可攜式媒體儲存裝置應予妥善保管，備份之儲存裝置應隔離儲存，可攜式儲存媒體、設備借用單如附件三。

七、凡列為機密等級之物品，非經核准不得攜出作業場所，已記錄有資料或程式之電腦作業媒體(包括磁碟、磁帶、磁片、光碟片、USB 隨身碟及報表等)及密碼等應嚴密控管。

八、電腦廠商對硬體設備實施維修時，為兼顧裝備安全及資料之完整性，應限制其工作地點，並指定專人隨時在旁，配合作業。

九、委託廠商開發軟體，對參與作業之人員，應先辦理查察，並確實瞭解其忠誠，對不合規定者，得拒絕其參與作業。

十、參與廠商的作業人員要求查閱機密資料前，應予嚴格審查，其調閱的適當性與否。

十一、密碼之強度及使用規範如下:

(一)禁止使用空白密碼。

(二)密碼長度至少為八個字元,管理者密碼至少為十個字元。

(三)密碼變更時,新密碼不得與前三次密碼相同。

(四)密碼設定應包括數字及英文字母,包括特殊字元。

(五)系統之密碼至少每 3 個月更換一次為原則。

(六)避免使用與個人有關資料(如生日、身分證字號、員工編號、電話號碼等)作為密碼。

(七)使用者密碼須妥善保管,避免他人知悉。

陸、電腦資料檔案分類

一、電腦檔案所含資料若認與公司營運或與個資法相關之項目者，列入限閱資料，其餘為普通資料，存取限閱資料檔案時，需將異動前後之資料、異動者帳號、異動時間等紀錄下來，並至少保存一年以上。

二、限閱資料檔案如下：

（一）申裝登記資料檔 ： 紀錄申請配管者姓名，地址及電話資料。

（二）改管資料主檔 ： 紀錄申請改管者姓名，地址及電話資料。

（三）分期付款檔 ： 紀錄用戶分期付款收據抬頭地址資料。

（四）供應商資料檔 ： 紀錄連絡人及電話等資料。

（五）承包商資料檔 ： 紀錄連絡人及電話等資料。

（六）工程發包主檔 ： 紀錄工程名稱(姓名)及地址等資料。

（七）完工用戶資料檔 ： 紀錄用戶名稱，地址及電話等資料。

（八）用戶基本資料主檔 ： 紀錄用戶名稱，地址，電話及銀行帳號等資料。

（九）用戶基本資料檔: 紀錄用戶名稱及地址資料。

（十）電子帳單資料檔: 紀錄姓名，電話及電子郵件信箱資料。

（十一）用戶安檢主檔: 紀錄用戶名稱，地址及電話資料。

（十二）人事基本資料檔: 紀錄姓名，身分證，生日，地址，電話，婚姻，教育及銀行帳號資料。

（十三）眷屬健保資料檔: 紀錄姓名，身分證，生日，地址資料。

柒、個人資料盤點及風險評估

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 2 款及第 3 款規定辦理，以界定各部室所保有之個人資料檔案，確實掌握期間內所保有之個人資料，並據以進行風險評估及管理，達成個人資料保護與管理之目標。

一 、個人資料盤點目的及作業程序：

（一）能有效清查及鑑別個人資料之名稱、類別(個資欄位)、保有依據、保有單位、特定目的、存在型態(書面/電子)、個資使用行為及相關利害關係人等。

（二）個人資料檔案盤點作業於每年 9 月底前執行完畢，並將盤點結果納入年度風險管理報告；另於組織變更或作業流程改變時，針對變動範圍內的作業程序與個人資料檔案進行個人資料檔案盤點作業。

（三）清查各作業流程中所使用之表單、紀錄，並辨識個人資料有關之表單、紀錄，歸納整理成個人資料檔案，將個人資料檔案檢視之成果製作個人資料檔案清冊，並妥善保管且定期維護該清冊，個資盤點表如附件四。

二、個人資料風險評估：

為評估個人資料檔案之風險，各部門應規劃個人資料風險評估與管理作業，風險評估作業應包括下列項目：

（一）鑑別個人資料所存在之各項衝擊及威脅所導致之風險，並依據風險評估之結果採取技術面及管理面之對策(接受、降低、轉移、迴避風險)或安全控制措施，以防止個人資料被竊取、竄改、毀損、滅失或洩漏。

（二）個資流程作業風險評估表 11 月底前完成彙整，並將結果納入年度

風險管理報告；另於營運組織變更、作業流程改變、新增或變更個人資料檔案、發生重大個資外洩事件時，針對變動範圍內的作業程序與個人資料檔案進行風險評估。

（三）建立風險評量的標準，包括風險發生的機率與衝擊之程度，並應依據實際狀況，從可識別性、個資數量、敏感程度、特定目的範圍內運用、外部利用、國際傳輸等六個評估構面進行風險分析。

（四）個資流程作業風險評估事項表如附件五。

（五）資通安全各部門自檢表如附件六、七。

（六）個人資料保護安全維護措施執行情形自我檢核表如附件八。

三、委外處理個資之責任因子

(一)挑選委外廠商或合作夥伴(受託人)時充分考量資安能力。

(二)確認所委託蒐集處理利用之個資範圍、類別、特定目的及其期間。

(三)確認受託人採取必要之個人資料檔案安全維護措施。

(四)有複委託者，確認其複委託之對象及確認複委託對象蒐集處理利用之個人資料之範圍、類別、特定目的及其期間。

(五)受託人或其受僱人違反個資保護法令或委託契約時，是否有向委託人通知之程序及確實通知。

(六)委託關係終止或解除時，是否要求受託人返還或銷毀因委託事項所交付之個資儲存媒體或紙本，及確認因委託事項所儲存於受託人處之個資確已刪除。

(七)以適當方式確認受託人具體執行前六點程序，並留存相關紀錄以供查驗。

(八)受託人之事故通報程序是否建立且留存相關紀錄。

捌、應變、通報及預防機制

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 4 款規定辦理，以使本公司保有之個人資料，於發生被竊取、竄改、毀損、滅失、洩漏等個資事故時，進行緊急事故應變處理。

一、採取之應變措施，包括下列事項：

(一)控制當事人損害方式。

(二)查明事故原因後通知當事人之方式(附件十)。

(三)通知當事人事故之事實、所為之因應措施及諮詢服務專線等內容。

二、受通報之相關對象及通報方式。

三、如屬用戶權益者，事故發生後研議預防措施。

因所保有之個人資料遭受竊取、竄改、毀損、滅失、洩漏或其他安全事故，致危及正常營運或大量當事人權益時，應於發現事故後七十二小時內，依附件十一格式以書面通報經濟部能源署。

經濟部能源署接受前項通報後，得依「電業及公用天然氣事業個人資料檔案安全維護管理辦法」第二十二條至第二十五條規定，為適當之監督管理措施。

四、事故通報：

獲報並經初步確認屬個資外洩之危機事件後，應立即以電話將訊息傳達至委員會執行秘書，並填寫個人資料事故通報單(附件九)，後續再由執行秘書通報至副召集人、召集人。

五、事故應變：

(一)應於接獲通報後 24 小時內進行事故分析。事故分析應包含確認事故之種類、事故嚴重程度、影響的範圍以及發生原因。

(二)於事故分析後，應研擬事故應變處理措施避免事故擴大，並採取證據保全措施，避免異動或改變原始磁碟及證據。

(三)於事故查明後，應即適當方式通知當事人被侵害之事實以及已採取之措施。適當方式得依個資法施行細則第 22 條規定為之。

六、媒體應對：

個資事故發生後，如輿論關注須對外說明及澄清，應由本公司發言人對外說明，不得臆測或對外講述不實言論。

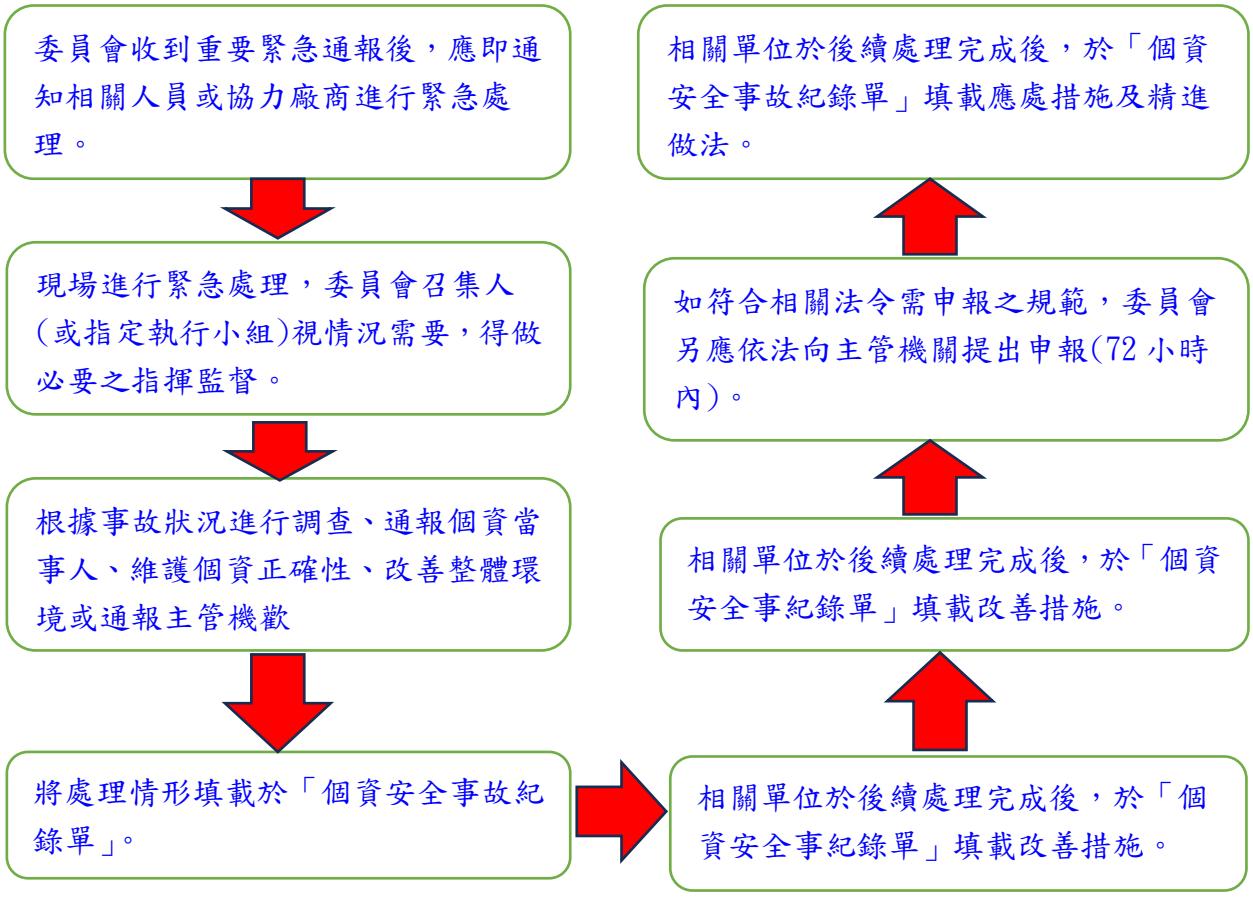
七、復原及預防

(一)經事故通報、事故應變、媒體應對之程序完成後，重新檢討事故發生之原因並擬定改善計畫；必要時，得重新進行風險評估及個人資料管理機制之設計。

(二)案發單位應將事故檢討及改善計畫，填寫個資安全事故紀錄單，並簽

陳召集人核定後，送交執行秘書備查；必要時，得由召集人召開制度檢視會議。

欣屏天然氣股份有限公司
個資安全事故之處理程序



玖、資料安全稽核程序

依據個資法第 18 條、個資法施行細則第 12 條第 2 項第 9 款及第 11 款規定辦理，以瞭解個資保護管理制度之實際執行狀況，並藉以瞭解相關缺失，並持續進行改善，使個資保護管理制度能夠更加完善，本公司由稽核組長進行個資保護作業稽核工作，稽核工作內容如下：

一、審查內部各部室之個資保護運作情形。

二、記錄並報告稽核結果，於每年 12 月底之前完成稽核作業，並製作個資管理稽核報告。

三、妥善保存稽核文件，並遵守保密規定。

四、追蹤改善措施。

拾、演練情境

為避免本公司因影響正常作業之運作與個人權益，進行個人資料侵害事故緊急應變模擬演練，以提高本公司同仁對個人資料安全管理警覺性；並強化熟悉本公司之緊急應變程序(如通報應變程序等作業)，使本公司之聲譽傷害降至最低、其日常作業能於最短時間內回復正常運作，以維護其作業之順暢與安全。每年度應演練情境乙次，並記錄備查。

情境一：

假想本公司有同仁將含有當事人個人資料（姓名、身份證字號、服務單位 、 薪資紀錄、員工編號）之資訊系統委託給某委外廠商進行維護 。惟承辦人員未依個資法善盡監督與管理之責，委外廠商人員藉此監督漏洞，藉由個人資料存取權限將個人資料進行網路販售，新聞媒體收到民眾舉報消息並披露本案，導致本公司個人資料保護形象受到質疑與面臨當事人向本公司提出損害賠償主張 。

情境二：

假想本公司部門同仁利用職務之便長期登入公司資訊系統，持續蒐集用戶個人資料（公司名稱、姓名、身份證字號、電話及聯絡方式），並且販售給保險業務員，用戶得知後向經濟部能源署檢舉，並向新聞媒體舉報且披露本案，導致本公司個人資料保護形象受損與面臨當事人向本公司提出損害賠償主張。

拾壹、一般規定

一、本計畫頒布後，3 日內即完成個資盤點，後續再依定期(每年 9 月)實施。

二、維護管理組織異動人員，以正式人令通知為主。

三、本計畫如有未周事宜，將滾動修進，另行訂定。

欣屏天然氣股份有限公司資訊安全暨個人資料保護委員會權責劃分表		
項次	職稱	職務內容
1	召集人 總經理	1.指導委員會所訂定之個資保護政策與個資保護全盤事宜。 2.主持個資相關會議。 3.協調委員會之委員意見。
2	執行秘書 業務經理	1.確認各部門執行個資保護聯絡窗口。 2.制定個資保護相關政策。 3.審核個資管理之相關配套計畫。 4.監督個資保護之相關計畫執行進度。 5.蒐整個資保護成效，納入風險管理運作情形報告。 6.持續改善個資保護機制。 7.因應主管機關之查核作業及緊急狀況通報。 8.回應個資當事人對個資之需求。 9.主導個資異常之應對策略及年度盤點作業。 10.制定盤點計畫。 11.制定與增修訂個人資料保護作業要點。 12.制定個人資料之風險評估以及應變管理機制。 13.進行個資宣導與教育訓練。
3	執行小組 各部(站)主管	1.督管業管之個資盤點。 2.進行個人資料之風險評估以及應變管理機制。 3.建立個資事故之預防、通報及應變機制。 4.執行委員會決議事項。 5.因應所有個資之異常現象及主管機關之查核作業 6.進行個資宣導與教育訓練。 7.通知個資當事人個資使用及異常處理情況。 8.指導緊急狀況處置，並回報執行秘書及召集人。 9.蒐整個資保護成效，納入風險管理運作情形報告
4	稽核小組(財務經理)	稽核個資作業是否符合個資法之規範
5	法律諮詢顧問團隊	提供相關法律諮詢及訴訟程序。
6	個資保護負責人 (個資保護聯絡窗口)	1.負責蒐集、處理、利用、存管及盤點營運必要之個人資料。 2.緊急狀況處置，並回報執行小組。
7	資訊組人員	1.導入必要且符合個資法規範之資安工具。 2.執行與個資法規範相關之資安防護與管制作業。
8	個資當事人(內、外部)	提出個資處理需求。
9	廠商/承裝商/承裝商	1.提供必要之資安工具及保密作為。 2.遵守委員會所制定之規範。
10	客戶/消費者	遵守委員會所制定之規範。
11	委外人員	遵守委員會所制定之規範。
12	全體員工	遵守委員會所制定之規範。

欣屏天然氣股份有限公司個資保護負責人 （個資保護聯絡窗口）			
部　室		負責人(聯絡窗口)	電話
管理部	經　理	蔡明樹	08-7532405#501
	秘書室	林文宗	08-7532405#304
工務部	經　理	何定奎	08-7532405#201
	設計組	李茂毅	08-7532405#204
	維護組	張嘉麟	08-7532405#208
財務部	經　理	李炳南	08-7532405#221
業務部	經　理	羅志銘	08-7532405#101
	組　長	廖倍香	08-7532405#104
東港 營業站	主　任	顏獻能	08-8356889

附件一

欣屏天然氣股份有限公司

資訊安全保密切結書

本人 _____ 將嚴守工作保密規定與國家相關法令對業務機密及客戶個人資料負完全保密之責，並尊重智慧財產權。絕不擅自洩漏、傳播職務上任何業務相關資料及任職期間經辦、保管或接觸之所有須保密訊息資料；絕不擅自複製安裝、傳播任何侵害智慧財產權之任何程式、軟體，如有違反情事，願依法負起相關刑事、民事及行政等法律責任。

聲明保證事項如下：

一、恪遵公司資訊安全規定，不私自蒐集或洩漏任何業務資訊，不得以任何形式，將上開資訊洩漏、複製、轉讓、再使用或交付公示於他人。

二、遵守「個人資料保護法」之規定，妥善收集、處理及利用客戶個人資料。

三、保密之義務，不因在職或離職而終止。

此致

欣屏天然氣股份有限公司

立 同 意 書 人：_____

中　　華　　民　　國　　年　　月　　日

附件二之一

委外廠商保密切結書

_____公司（以下簡稱乙方）受欣屏天然氣股份有限公司（以下簡稱甲方）委託辦理「_____案」（以下簡稱本專案），乙方執行本專案接觸之公務（機密）資料，具結依下列規定保密並履行責任：

一、 乙方於本專案進行期間因進行調查、搜集依合約所產生或所接觸之業務（機密）資料，非經甲方同意或授權，不得以任何形式洩漏或將上開資料再使用或交付第三者。對所獲得或知悉之上述業務（機密）資料，乙方須負保密責任。

二、 業務（機密）資料保密期限，不受本專案工作完成（結案）或合約到期及乙方不同工作地點及時間之限制，乙方持有或獲知業務（機密）資料，未經甲方書面同意或授權，不得洩漏或轉讓於第三者。

三、 乙方違反資訊安全保密切結書之規定，致造成甲方或第三者之損害賠償，乙方同意無條件負擔全部責任，包括因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。於第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方應合作提供絕無異議。

此致

欣屏天然氣股份有限公司

具切結書廠商：_____（公司章）

代 表 人：_____

統 一 編 號：_____

公 司 地 址：_____

電 話：_____

本公司蒐集本表單上所列之個人資料，作為辨識您為簽署本保密切結書之本人，並為追溯違反本保密切結相關規定用途，不做其他目的範圍外之利用，並遵循個人資料保護法與本公司個資保護之要求辦理。

中　　華　　民　　國　　年　　月　　日

附件二之二

委外廠商人員保密切結書

立切結書人＿＿＿＿＿＿（以下簡稱乙方）參與欣屏天然氣股份有限公司（以下簡稱甲方）辦理「＿＿＿＿＿＿＿＿＿＿案」，工作期間因業務需要接觸之業務（機密）資料，乙方願意依下列規定辦理：

一、乙方於專案進行期間因進行調查、蒐集依合約所產生或所接觸之業務（機密）資料，不得以任何形式洩漏或將上開資料再使用或交付第三者。對所獲得或知之上述業務（機密）資料，乙方須負保密責任。

二、業務（機密）資料保密期限，不受專案工作完成（結案）或合約到期及乙方不同工作地點及時間之限制。乙方持有或獲知業務（機密）資料，不得洩漏或轉讓於第三者。

三、乙方違反本資訊安全保密切結書之規定，致造成甲方或第三者之損害或賠償，乙方同意無條件負擔全部責任，包括因此所致甲方或第三人涉訟，所須支付之一切費用及賠償。於第三人對甲方提出請求、訴訟，經甲方以書面通知乙方提供相關資料，乙方應合作提供，絕無異議。

此致

欣屏天然氣股份有限公司

立切結書人：＿＿＿＿＿＿

姓　名：＿＿＿＿＿＿＿＿

地　址：＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿＿

本公司蒐集本表單上所列之個人資料，作為辨識您為簽署本保密切結書之本人，並為追溯違反本保密切結相關規定用途，不做其他目的範圍外之利用，並遵循個人資料保護法與本公司個資保護之要求辦理。

中　　華　　民　　國　　年　　月　　日

附件三

欣屏天然氣股份有限公司
可攜式儲存媒體、設備借用單

申請日期：

申請人		申請部門	
借用設備			
是否攜出該設備			
預計借用時間		預計歸還時間	
借用原因			
實際借用時間		實際歸還時間	
備註			

部門主管　　總經理

資訊主管

附件四　個資盤點事項表(範例)

單位名稱	
單位主管	
盤點人員	

主要業務、職掌	細部作業名稱	個人資料檔案名稱	主管單位	保有單位	檔案形態	保有依據	是否需告知	特定目的	個人資料類別	§17 對外公告
○○○業務推動	○○○作業	○○○	經濟部能源署	○○部	■紙本 □電子類 □電子檔-可攜式媒體 □系統資料庫	個資法第○條	■Y □N	發展業務需要	C○三一(住家及設施)	□Y ■N

資料來源	內部傳送	外部傳送	委外	個人資料項目	特種個人資料	保管方式	保存期限	銷毀方式	備註	單位名稱
當事人自行提供	○○組	無	無	■姓名 □生日 ■身分證號 □護照號碼 □特徵 □指紋 □婚姻 □家庭 □教育 □職業 ■聯絡方式 □財務情況 □社會活動 □其他：_____	■無 □病歷 □醫療 □基因 □性生活 □健康檢查 □犯罪前科	放置於辦公室檔案櫃並鎖上	□法定保存期限：____ □自訂保存期限：____	保存期限屆滿後由○○部統一辦理銷毀作業	N/A	○○部

項目	填寫說明
主要業務、職掌	依單位業務、職掌內容、業務項目等，列出主要的作業流程名稱。
細部作業名稱	前項作業流程名稱，依其日常的辦理流程，再個別區分成細部作業。
個人資料檔案名稱	包含可識別當事人之個人資料檔案名稱。
主管單位	負責制定該個人資料檔案項目與欄位之部門。(業務主管部門或個資檔案之規劃部門)
保有單位	保存及管理個人資料檔案之部門。
檔案形態	檔案型態分為下列四種： 1.紙本類：指實體紙本文件。 2.電子類：包含報表、文件掃描檔、照片、圖片、傳真、影像檔等相關電子文件檔案，如 WORD、EXCEL、PDF、WMV 等數位型式之檔案。 3.電子檔-可攜式媒體：指上述數位形式文件保存於可攜式媒體。 4.系統資料庫：指個人資料僅保存於資訊系統內，未另外列印成紙本或另存成電子檔案。 需分筆列示於個人資料盤點清冊。
保有依據	是否有法定保有依據或契約或機關自定之保有依據。
是否需告知	請判斷是否需依個資法第 8 條及第 9 條規定，蒐集、處理或利用個人資料時應明確履行告知義務。 如需告知，請填 Y；得免為告知，請填 N。
特定目的	依法務部公告之「個人資料保護法之特定目的及個人資料之類別」填寫個人資料蒐集或處理之特定目的。
個人資料類別	依法務部公告之「個人資料保護法之特定目的及個人資料之類別」填寫個人資料類別。
§17 對外公告	請判斷該個人資料檔案是否依個資法第 17 條規定,對外公告個人資料檔案名稱、類別、特定目的、保有依據等必要

	項目。 如需對外公告，請填 Y；若無需公告，請填 N。
資料來源	該個人資料檔案取得管道或建立之方法。
內部傳送	與該個人資料檔案之蒐集、處理或利用有關之內部部門。
外部傳送	與組織之個資檔案提供外部利用有關，本項指無法歸屬於本機關之單位或人員等。
委外	提供之服務與個資檔案之蒐集、處理及利用流程有關，且會接觸到個資內容之委外機(構)或人員。
個人資料項目	姓名、生日、身分證號碼、護照號碼、特徵、指紋、婚姻、家庭、教育、職業等。
特種個人資料	病歷、醫療、基因、性生活、健康檢查、犯罪前科。
保管方式	該個人資料檔案之保管方式(如：放置於辦公室檔案櫃並上鎖、儲存於承辦人電腦並將檔案加密、資料庫主機...等)。
保存期限	法定保存期限：該個人資料檔案依據檔案法等相關法律規定之保存期限(如：3 年、5 年...等)，並請說明法定依據。 自訂保存期限：該個人資料檔案依據本機關自訂之保存期限(如：3 年、5 年...等)。
銷毀方式	該個人資料檔案之銷毀方式(如：由總務單位統一辦理銷毀作業...等)。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。

附件五　個資流程作業風險評估事項表

項目	填寫說明
主要業務、職掌	依個資流程衝擊之分析類別「主要業務、職掌」欄位填寫。
細部作業名稱	依個資流程衝擊之分析類表「細部作業名稱」欄位填寫。
風險大分類	依「細部作業名稱」囊括之個人資料檔案形態填入，詳細內容請考量風險情境事項。 若「細部作業名稱」囊括之個人資料檔案含委外作業，則需加入委外作業類。
風險子分類	依前欄之風險大分類展開風險子分類逐一填入，詳細內容請考量風險情境事項。
個資檔案控管措施(風險情境)	依前欄之風險子分類展開該類別風險情境，詳細內容請考量風險情境事項。
衝擊值	從個人資料衝擊分析類別將衝擊值納入考量。
個資侵害風險發生可能性評估	以「個資侵害風險發生可能性」欄位所述級距進行評估。 於受評估之個資作業流程中，該風險情境不存在者，填「0」(不適用)。
風險值	個資作業流程衝擊值x風險發生可能性。
備註	任何可補充說明的資訊。
單位名稱	個資檔案所屬之單位名稱。

單位名稱	
單位主管	
評估人員	

作業流程名稱		風險控管分類			衝擊值(A)	個資侵害風險發生可能性(B)	風險值	備註	單位名稱
主要業務、掌職	細部作業名稱	風險大分類	風險子分類	個資檔案控管措施(風險情境)	從個人資料衝擊分析衝擊帶將值擊表入	5：控管嚴謹度低、經常被忽略、現行個資檔案控管方式沒有詳細規範。	風險值=個資作業流程衝擊值(A)×風險發生可能性(B)		
						3:控管嚴謹度中等、偶發性被忽略、現行個資檔案控管方式僅有部分規範。			
						1：控管嚴謹度高、充分落實，現行個資檔案控管方式已有詳細規範。			
						0：不適用			

個資流程作業風險評估表

作業流程名稱		風險控管分類			衝擊值(A)	個資侵害風險發生可能性(B)	風險值	備註	單位名稱
主要業務、職掌	細部作業名稱	風險大分類	風險子分類	個資檔案控管措施(風險情境)	從個人資料衝擊分析表將衝擊值帶入	5：控管嚴謹度低、經常被忽略、現行個資檔案控 3：控管嚴謹度中等、偶發性被忽略、現行個資檔案控管方式僅有部分規範。 1：控管嚴謹度高、充分落實，現行個資檔案控管方式已有詳細規範。 0：不適用	風險值=個資作業流程衝擊值(A)×風險發生可能性(B)		
○○○業務之規劃、推動	○ ○ ○作業	1.紙本類	1.1處理	1.1.1 紙本文件於內部處理過程中，長時間不使用或下班時收存於辦公室上鎖之	12	1	12	N/A	○○部
○○○業務之規劃、推動	○ ○ ○作業	1.紙本類	1.2保存	1.2.1 紙本文件之保存(含暫存區)地點具備進出管控措施。	12	3	36	N/A	○○部
○○○業務之規劃、推動	○ ○ ○作業	1.紙本類	1.2保存	1.2.2 紙本文件歸檔、入倉(庫)或集中保管前，確實清點數量及內容。	12	1	12	N/A	○○部
○○○業務之規劃、推動	○ ○ ○作業	1.紙本類	1.2保存	1.2.3 紙本文件存放地點有消防、滅火、溫度控制等設施。	12	3	36	N/A	○○部

附件六

欣屏天然氣股份有限公司
資通安全各部門自檢表

檢查日期:

檢查項目	描述	檢查結果	說明
電腦使用管理	1. 公司配發的電腦及設備僅進行與工作相關的活動。	□ 是 □ 否	
	2. 未經許可不得將電腦設備借予他人使用。	□ 是 □ 否	
	3. 未經許可不得使用 USB 於公司配發電腦或設備。	□ 是 □ 否	
電腦資產管理	1. 不得自行進行作業系統重置或軟體移除。	□ 是 □ 否	
	2. 不得自行拆卸或更換硬體零件。	□ 是 □ 否	
	3. 不得擅自安裝未經授權軟體。	□ 是 □ 否	
網路使用管理	1. 確保員工上班使用網路資源與工作相關。	□ 是 □ 否	
	2. 確保員工無利用公司資源從事不法行為或導致他人損害。	□ 是 □ 否	
	3. 私人電腦及非公司人員設備使用公司資源上網前，需先經主管同意。	□ 是 □ 否	
	4. 不得使用公司網路至來源不明或非法的網站。	□ 是 □ 否	

檢查項目	描述	檢查結果	說明
資料保密管理	確保電腦使用人對電腦中的資料負有保管和保密的責任。	□ 是 □ 否	
帳號使用	不得任意將帳號密碼借予他人使用。	□ 是 □ 否	
信箱使用規定 檔案存取管理	1. 不得發送大量與工作無關的郵件。	□ 是 □ 否	
	2. 不得發送非法、威脅性或未經授權的資料。	□ 是 □ 否	
	3. 未經許可不得任意使用外部郵箱帳號。	□ 是 □ 否	
	4. 不得開啟來源不明的檔案或未經授權的電子郵件連結。	□ 是 □ 否	
	5. 未經許可不得將工作相關檔案轉為私人用途或以任何形式轉送置工作外部。	□ 是 □ 否	
	6. 刪除檔案前，確認該檔案是否已過期或不再需要。	□ 是 □ 否	
	7. 修改檔案前，確保修改是基於工作需要且經過相關授權。	□ 是 □ 否	
	8. 僅在必要情況下複製檔案，並確保複製檔案僅用於工作用途。	□ 是 □ 否	

附件七

欣屏天然氣股份有限公司
資通安全資訊室自檢表

檢查日期:

檢查項目	描述	檢查結果	說明
帳號申請	1. 正式員工申請郵件帳號時，確認是否填寫申請表格，並確保申請表格完整。	□是 □否	
	2. 確認是否有對於約聘人員的申請和授權流程，以及管理部門是否已經同意。	□是 □否	
帳號使用	1. 檢查公司郵箱帳號是否只用於工作相關事項，避免個人用途。	□是 □否	
	2. 確保員工明白保管好自己的帳號和密碼，禁止將密碼借給他人使用。	□是 □否	
信箱使用規定	1. 檢查員工是否定期檢查信箱空間，及時處理舊郵件。	□是 □否	
	2. 確保員工不得開啟來源不明或未經授權的電子郵件連結。	□是 □否	
信箱安全性	1. 確保員工不發送非法、威脅性或未授權的資料。	□是 □否	
	2. 檢查是否有人發送大量與工作無關的郵件。	□是 □否	
	3. 確認公司是否對所有郵件進行了備份和監控，以保障安全性和合規性。	□是 □否	
郵件系統管理	確保公司內部禁止使用外部郵箱帳號。	□是 □否	
檔案存取管理	1. 檔案存取僅限於工作相關，禁止轉為私人用途或以任何形式轉送至公司外部。	□是 □否	
	2. 確保新增檔案僅涉及工作相關內容，並遵循公司檔案管理政策。	□是 □否	
	3. 刪除檔案前，確認該檔案是否已經過期或不再需要，避免誤刪。	□是 □否	
	4. 修改檔案時，確保修改是基於工作需要並經過相關授權。	□是 □否	
	5. 僅在必要情況下複製檔案，並確保複製的檔案僅用於工作用途。	□是 □否	
智慧財產保護	1. 確保尊重智慧財產權，不任意修改、刪除、複製他人文件、程式或技術資料。	□是 □否	

檢查項目	描述	檢查結果	說明
	2. 嚴格遵守公司文件管理政策，不得隨意更改或刪除文件，保護公司和他人的知識產權。	□是 □否	
檔案存取權限	確保存取他人文件時擁有相應的權限，不得濫用權限存取非負責或擁有文件。	□是 □否	
檔案保密性	確保所有檔案存取及相關記錄的保密性，僅限授權人員查閱。	□是 □否	
電腦資產管理	1. 確保不自行進行作業系統重置或軟體移除，以免資產損壞。	□是 □否	
	2. 確保不拆卸或更換硬體零組件，保持電腦完整性。	□是 □否	
	3. 確保所有安裝軟體均為授權軟體，不得擅自安裝未經授權的軟體。	□是 □否	
	4. 確保配發的電腦中的資料所有權為公司所有。	□是 □否	
	5. 確保定期對電腦中相關資料進行備份及存取動作，以防資料丟失或損壞。	□是 □否	
電腦使用管理	1. 確保員工使用配發的電腦及設備僅進行與工作相關的活動。	□是 □否	
	2. 確保未經許可不得將電腦設備借予他人使用。	□是 □否	
	3. 確保員工未經許可不得使用 USB 於公司配發電腦或設備。	□是 □否	
資料保密管理	確保電腦保管人對電腦中的資料負有保管和保密的責任，不得外泄公司敏感資料。	□是 □否	
網路連接管理	1. 確保公司配置的個人電腦需經資訊室設定後方可連接網際網路，以確保安全性。	□是 □否	
	2. 私人電腦及非公司人員之設備使用公司資源上網前，需獲得主管許可並由資訊室進行相關設定後方可連線上網，以保障資料安全。	□是 □否	
	3. 確保非經資訊室同意，不得以數據機或其他方式繞過公司防火牆直接存取網際網路，以維護系統安全性。	□是 □否	
網路使用管理	1. 確保員工上班使用網路資源與工作相關，並根據公司政策限制部分網站的訪問，如股票、色情網站等。	□是 □否	

檢查項目	描述	檢查結果	說明
	2. 系統管理人員發現使用異常時，可緊急將設備離線或暫時阻斷存取，以維護公司資源使用的正常，並通知當事人後再視情形恢復。	□是 □否	
	3. 若發現員工利用公司資源從事不法活動或違反公司規定，處理人員應將記錄留存並通知相關單位進行處理。	□是 □否	
	4. 公司保留使用、統計、過濾、備份及內容側錄等權利，並根據公司政策限制網路存取範圍、頻寬等事項。	□是 □否	
	5. 員工使用公司系統從事不法行為或導致他人損害時,應自行承擔法律責任。	□是 □否	
	6. 對廠商訪客使用自帶筆電上網，僅能使用訪客專用的無線網路，不得使用公司內部有線網路上網，以避免資安風險。	□是 □否	
	7. 確保員工不得使用公司網路至來源不明或非法的網站。	□是 □否	

附件八

個人資料保護安全維護措施執行情形自我檢核表

公司名稱	欣屏天然氣股份有限公司
自我檢核日期	
自我檢核人員	

自我查核項目	自我評估結果			佐證資料及說明
	符合	不符合	不適用	
一、配置管理之專責人員及相當資源				
1.是否建立個人資料檔案安全維護管理組織？				
2.是否定期召開個人資料檔案安全維護管理組織會議？				
3.是否配置適當人員及資源？				
4.是否建立個人資料檔案安全維護計畫及業務終止後個人資料處理方法？				
5.承上，是否經代表人或其授權之人核定並發布？				
6.承上，是否備置於總機構及營業處所？				
7.個人資料檔案安全維護管理組織是否定期提出書面評估報告？				
二、界定個人資料之範圍				
1.蒐集、處理或利用顧客之個人資料是否達 3,000 筆以上？				
2.是否定期進行個資盤點？				
3.個資盤點是否確實？				
4.負責個資盤點人員是否定期接受個資盤點相關教育訓練？				
三、個人資料保護之風險評估及管理機制				
1.是否建立風險管理機制？				
2.是否定期進行風險評估？				
3.是否針對風險評估結果提出因應機制？				
四、事故之應變、通報及預防機制				
1.是否制訂事故之應變、通報及預防機制				
2.是否制訂查明事故原因後，通知當事人之方式？				
3.是否建立通知當事人因應措施之諮詢服務專線？				

4.事故發生時是否有通報之相關對象及通報方式？				
5.是否訂定事故發生後之預防措施？				
五、個人資料蒐集、處理及利用之內部管理程序				
1.是否建立個人資料蒐集、處理及利用之內部管理程序？				
2.個人資料之蒐集、處理或利用，是否符合免為告知之事由，及所告知之內容、方式是否合法妥適？				
3.個人資料之蒐集或處理，是否具有個人資料保護法第 19 條規定具有特定目的及法定情形？				
4.個人資料之蒐集或處理，是否有逾越個人資料保護法第 19 條所稱「特定目的」之情形？				
5.個人資料之利用，是否符合個人資料保護法第 20 條規定蒐集之特定目的必要範圍或法定情形？				
6.個人資料之利用，有無於特定目的必要範圍外利用之情形？				
7.利用個人資料為行銷，是否提供當事人免費表示拒絕接受行銷之方式？				
8.就個資之蒐集、處理或利用是否委託第三人執行？				
9.如有，是否將受委託廠商義務及違反義務之罰則明訂於委託契約或相關文件中？				
10.是否定期確認複委託廠商個資作業之執行狀況？				
11.是否建立複委託廠商或其人員違反個資法或合約時之通報機制？				
12.是否建立當事人就其個人資料行使個人資料保護法第 3 條權利之相關流程機制？				
13.有無定期檢視個人資料於蒐集、處理或利用過程中是否正確？				
14.有無定期檢視所保有個人資料之特定目的是否消失，或期限是否屆滿，並刪除、停止處理或利用？				
六、資料安全管理及人員管理				
1.是否訂定各類設備或儲存媒體之使用規範？				
2.各類設備或儲存媒體報廢或轉作他用時，是否採取適當防範措施？				
3.蒐集、處理或利用有加密需要之個人資料內容，是否採取適當加密機制？				
4.是否對個人資料之備份資料採取適當保護措施？				
5.是否妥善保存認證機制及加密機制中所運用之密碼？				
6.是否以資通訊系統蒐集、處理或利用個人資料，且保有數量達一萬筆？				

7.如有，是否有建立相關個資保護機制？				
8.是否依據所屬人員業務特性、內容及需求，設定不同權限？				
9.是否定期檢視所屬人員權限內容之適當性，並控管接觸個人資料之情形？				
10.是否與所屬人員就接觸之個人資料約定保密義務？				
七、認知宣導及教育訓練				
1.是否對既有員工及新進人員定期進行個資保護認知宣導與教育訓練？				
2.是否留存教育訓練之紀錄？				
八、設備安全管理				
1.對於保有個人資料之設備，是否依據業務特性、內容及需求，實施適當進出管制？				
2.是否安裝防毒軟體並定期更新病毒碼？				
3.是否訂定妥善保管個人資料儲存媒介物之方式？				
4.是否依媒介物之特性、使用方式及其環境，建置適當保護設備或技術？				
5.刪除、停止處理或利用所保有之個人資料後，是否保存其方法、時間、地點及證明方式？				
6.將前述資料移轉他人時，是否記錄移轉之原因、對象、方法、時間、地點及受移轉對象得蒐集、處理或利用該個人資料之合法依據？				
九、資料安全稽核機制				
1.是否定期執行個資保護稽核作業？				
2.是否針對稽核結果提出並執行改善計畫？				
3.是否留存稽核及改善程序執行之紀錄？				
十、使用紀錄、軌跡資料及證據保存				
1.是否留存提供當事人行使權利之紀錄？				
2.是否留存備份及還原測試之紀錄？				
3.是否留存所屬人員權限新增、變動及刪除之紀錄				
4.是否留存因應事故發生所採取行為之紀錄？				
5.是否留存個資系統之定期檢查紀錄？				
十一、個人資料安全維護之整體持續改善				
1. 個人資料檔案安全維護管理組織是否持續改善個人資料安全維護？				
2.是否定期檢視評估報告，並針對有違反法令情形之虞者，規劃、改善並提出預防措施？				

附件九　　個人資料事故通報單

<table>
<tr><td>通報單位</td><td colspan="2"></td><td>通報時間</td><td colspan="2">年　　月　　日
時　　分</td></tr>
<tr><td>個資事故
說明</td><td colspan="5">一、個資事故發生與發現之日期與時間：

二、洩漏單位
□ 本公司洩漏
□ 委外廠商洩漏

三、遭受揭露之個資範圍與敘述：(如：個人資料檔案名稱、個人資料類別及個人資料數量等)

四、遭受揭露個資之儲存媒體：(如：紙本、電子檔案、系統資料庫、光碟片、USB碟、可攜式硬碟或記憶卡等)</td></tr>
<tr><td>受理人
(資訊室)</td><td colspan="2"></td><td>受理時間</td><td colspan="2">年　月　日
時　分</td></tr>
<tr><td>事故分析
及判定</td><td colspan="5">經初步分析後判定為：
□ 個資事故/事故權責單位名稱：
□ 疑似個資事件（持續觀察，暫不處理）
□ 非個資事件　（不處理，逕行結案）
說明：

□是□否 需向律師事務所/廠商尋求支援</td></tr>
<tr><td>事故單位
承辦人</td><td>事故
單位主管</td><td colspan="2">執行秘書</td><td colspan="2">批示</td></tr>
<tr><td></td><td></td><td colspan="2">資訊組長</td><td colspan="2">召集人</td></tr>
</table>

附件十　　通知當事人文稿(範例)

○○○先生(女士) 您好：

茲因欣屏天然氣股份有限公司(以下簡稱本公司)「○○系統」遭植入惡意後門程式,致使台端之個人資料遭駭客竊取並公布於○○上，經調查確認本案確為個人資料外洩事故。

本公司對此一事故極為重視，特說明本次事故之處理，以化解台端之疑慮。

1、台端之個人資料因本部網站遭駭客植入惡意程式導致外洩，影響您的隱私權益，依個人資料保護法規定，本公司需通知您有關本案之實際情況及本部已採取之因應措施。

2、(此案例為系統遭駭客入侵導致個人資料外洩,因應措施可參考下述說明)本公司業已進行 APT 惡意程式掃描,移除被植入之後門程式，並將網站程式重新上架，另已通知 Google 公司移除其搜尋引擎所儲存之快取資料，……，以避免您登錄於本部系統的個人資料再次被搜尋到。

3、若台端仍有疑慮，可與本公司○○○聯絡，聯絡電話：○○○-○○○○，將由專人為您說明及釋疑。

本公司對此次事件造成台端之困擾，再次致上歉意。本公司必記取此次事件之經驗,將再加強網站程式之安全性檢測，並強化資訊系統程式開發過程之安全性管理,確保類似事件不再發生，以保護個資當事人之隱私與權益。

中　華　民　國　○　年　○　月　○　日

欣屏天然氣股份有限公司個資安全事故通知當事人紀錄單			
通知日期		通知部門 人員	
個資安全事件 發生日期時間			
通知內容	個資被侵害之事實：		
	已採取之因應措施：		

受通知當事人	通知方式
○○○	電話、簡訊通知
○○○	郵件通知
○○○	電話、簡訊通知
○○○	郵件通知
○○○	電話、簡訊通知
○○○	郵件通知
○○○	電話、簡訊通知

附件十一　經濟部能源署-非公務機關個資外洩通報表

附表 非公務機關個資外洩通報表

<table>
<tr><td colspan="3">個人資料侵害事故通報與紀錄表</td></tr>
<tr><td>非公務機關名稱

通報機關</td><td colspan="2">通報時間：　年　月　日　時　分
通報人：　　簽名(蓋章)
職稱：
電話：
Email：
地址：</td></tr>
<tr><td>事件發生時間</td><td colspan="2"></td></tr>
<tr><td>事件發生種類</td><td>☐竊取
☐洩漏
☐竄改
☐毀損
☐滅失
☐其他侵害事故</td><td>個資侵害之總筆數(大約)

☐一般個資_____筆
☐特種個資_____筆</td></tr>
<tr><td>發生原因及事件摘要</td><td colspan="2"></td></tr>
<tr><td>損害狀況</td><td colspan="2"></td></tr>
<tr><td>個資侵害可能結果</td><td colspan="2"></td></tr>
<tr><td>擬採取之因應措施</td><td colspan="2"></td></tr>
<tr><td>擬採通知當事人之時間及方式</td><td colspan="2"></td></tr>
<tr><td>是否於發現個資外洩後72小時內通報</td><td colspan="2">☐是　☐否，理由</td></tr>
</table>