

水利署臺北水源特定區管理分署

委外安全管理程序書

V2.0

文件編號	WRA10-ISMS-2-006
分類等級	內部使用
初版日期	
修訂日期	

制訂	審查	會辦	核准

本文件為水利署臺北水源特定區管理分署所有，禁止翻印

文件編修紀錄

發行／修訂 版本	發行／修訂 生效日期	發行/修訂內容說明	制訂	審查	核准	備註
V1.0		為辦理本局各課室資訊化資料委外服務，建立本程序書初稿。		資通安全執行秘書	資通安全處理小組召集人	
V2.0		機關 112 年 9 月組織改造後名稱修正、內文、分類修訂		資通安全執行秘書	資通安全處理小組召集人	

目錄

0.	目的	4
1.	範圍	4
2.	相關文件	4
2.1	WRATB-ISMS-2-010 資通系統安全管理程序書	4
2.2	資通安全管理法施行細則	4
2.3	水利署及所屬機關資訊相關系統開發與維護注意事項	4
2.4	個人資料保護法施行細則	4
3.	作業說明	4
3.1	名詞定義	4
3.2	角色與權責	4
3.3	選任委外廠商	5
3.4	制定委外契約	5
3.5	委外廠商管理	6
3.6	委外廠商監督	6
4.	產出紀錄	7
4.1	委外廠商契約	7
4.2	WRATB-ISMS-4-016 委外廠商執行人員保密切結書	7
4.3	WRATB-ISMS-4-017 委外廠商執行人員保密同意書	7
4.4	WRATB-ISMS-4-018 委外廠商稽核項目表	7

0. 目的

為辦理水利署臺北水源特定區管理分署(以下稱本分署)各科室資通服務委外作業時，如：技術服務提供、硬體建置與維護、軟體建置與維護…等，有所依循或遵循，特訂定本程序書。

1. 範圍

1.1 本分署提報之核心資通系統及重要系統之委外廠商。

1.2 本分署基礎環境設施之委外廠商。

2. 相關文件

2.1 WRATB-ISMS-2-010 資通系統安全管理程序書

2.2 資通安全管理法施行細則

2.3 水利署及所屬機關資訊相關系統開發與維護注意事項

2.4 個人資料保護法施行細則

3. 作業說明

3.1 名詞定義

3.1.1 個人資料

泛指自然人之姓名、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、社會活動等。

3.2 角色與權責

3.2.1 各科室

3.2.1.1 辦理委外廠商選任及擬定委外廠商契約。

3.2.1.2 要求委外廠商簽定保密切結書及保密同意書，並要求遵守相關保密規定。

3.2.1.3 督導與管理委外服務，以滿足契約要求及符合法令、法規之要求。

3.2.2 委外廠商

3.2.2.1 遵守契約、保密切結書及保密同意書中之相關保密要求。

3.2.2.2 按照契約要求，執行相關作業活動，並接受監督或稽核。

3.2.2.3 遵守本分署資通安全管理制度的要求，執行相關作業。

3.3 選任委外廠商

3.3.1 各科室辦理資通服務委外，在進行選任委外廠商時，應遵守「資通安全管理法施行細則」第四條之規定辦理。

3.4 制定委外契約

3.4.1 各科室於擬定委外廠商契約時，須注意下列事項：

3.4.1.1 委外契約內容可以包括工作目標、工作項目、工作特性、工作量、時程、資訊環境、專案變更、驗收事項、雙方權責、付款方式、違約罰則等。

3.4.1.2 契約應依據委外服務內容，說明資通安全相關條款。

3.4.1.3 契約中應載明本分署保有自行或與第三方稽核單位，針對委外廠商稽核之權利。

3.4.1.4 契約中應要求委外廠商交付相關之文件，如：系統需求及規格書、軟硬體變更程序、系統文件、安裝/操作手冊及教育訓練。

3.4.1.5 契約中應明定委外廠商應交付之產品維護保固之期間、範圍、項目及費用計算標準。

3.4.1.6 契約中應明訂軟體之原始碼及執行碼之所有權及其他相關之智慧財產權之歸屬。

3.4.1.7 契約中應明定違反相關之資通安全規範，如情節重大者須負擔相關之法律責任及契約內簽訂之相關罰責。

3.4.1.8 如遇委外廠商需將服務或產品給其他廠商支援時，應要求主廠商書面化說明相關下包廠商之間的權責關係(可於契約本文描述或作為契約附件)，用以確保委外廠商之整體服務交付品質，並應要求其下包廠商遵守本分署資通安全管理制度。

3.4.1.9 委外廠商於契約內所建立經核准使用之系統帳號及權限、網路設定、資訊設備、文件資訊等，均需於契約或專案結束後確認清除或歸還。

3.4.1.10 委外事項如涉及應用系統開發與維護，應遵守「水利署及所屬機關資訊相關系統開發與維護注意事項」及「WRATB-ISMS-2-010 資通系統安全管理程序書」之規定辦理。

3.4.1.11 委外廠商應配合資通安全事件之通報及處理，並視需要參加資安訓練、個人資料保護相關課程與資通安全事件演練。

3.4.1.12 契約中應明定委外廠商指定單一窗口，負責專案進度與其他工作事項之聯繫。

3.4.1.13 契約中應說明例外情況（如：變更、轉讓、履約等）及其相關處置方式。

3.4.1.14 契約中應說明本分署與委外廠商間相關之責任與義務。

3.4.1.15 委外廠商應視需求請主辦科室召開專案工作會議，並產出專案執行進度及檢討報告。

3.4.1.16 契約中應說明撥付委外廠商契約價金之方式及條件。

3.5 委外廠商管理

3.5.1 委外廠商與其人員於提供本分署資通服務時，皆應簽署「WRATB-ISMS-4-016 委外廠商執行人員保密切結書」及「WRATB-ISMS-4-017 委外廠商執行人員保密同意書」，並遵守相關保密規定。

3.5.2 委外廠商於非上班時間需至本分署作業時，應事先告知本分署人員，以利管控人員出入。

3.5.3 委外廠商不得存取未經授權的資訊資產。

3.5.4 委外廠商應遵守本分署資通安全管理制度的規定，執行相關作業活動。

3.6 委外廠商監督

3.6.1 各科室權責人員應依據契約規劃的執行時程定期監督或不定期稽核委外廠商工作是否符合契約規範。

3.6.2 各科室執行委外廠商稽核作業時，可參考使用「WRATB-ISMS-4-018 委外廠商稽核項目表」，對於委外廠商進行稽核。

3.6.3 各科室權責人員於監督委外廠商時，應遵守「資通安全管理法施行細則」第四條之規定辦理。

3.6.4 若委外服務中涉及個人資料蒐集、處理或利用等作業，各科室權責人員於監督委外廠商時，除上揭 3.6.1~3.6.3 要求外，應遵守「個人資料保護法施行細則」第八條之規定辦理。

4. 產出紀錄

4.1 委外廠商契約

4.2 WRATB-ISMS-4-016 委外廠商執行人員保密切結書

4.3 WRATB-ISMS-4-017 委外廠商執行人員保密同意書

4.4 WRATB-ISMS-4-018 委外廠商稽核項目表