「WebITR 全國共享版機關內部差勤系統」
安裝暨使用規範

版本:1.0 日期:113年4月10日

一、 行政院人事行政總處(以下簡稱本總處)開發之「全國共享版機關內部差勤系統」（以下簡稱 WebITR）係以協助機關差勤管理為目的，其預設使用情境為機關內部使用，為提升 WebITR 之資通安全防護能力，特訂定本使用規範。

二、 本規範所指之 WebITR 安裝機關係指實際可管理 WebITR 主機之機關，WebITR 使用機關係指以 WebITR 作為其差勤管理系統之機關。

三、 WebITR 安裝機關因業務需要開放同仁透過網際網路使用，應建立包含但不限於以下之防護措施：

(一) WebITR 網路環境設定

1. WebITR 主機務必以 Web 應用程式防火牆(WAF)防護，並採用資安監控中心(SOC)監控網路封包傳輸狀況。
2. 禁止使用者透過境外 IP 存取 WebITR。
3. 系統之登入應採行來源驗證，切勿直接將 WebITR 開放任何 IP 透過網際網路存取。建議來源驗證可由以下方式擇一使用：
   - 限制僅有白名單所列之 IP 可登入 WebITR。
   - 限制僅能以 VPN 方式登入 WebITR。
   - 結合機關單一簽入機制(SSO)登入 WebITR ，並關閉 WebITR 之帳號密碼登入頁面。
   - 其他限制登入 WebITR 之管理方式(如單一簽入結合一次性密碼[OTP])。

(二) WebITR 主機安全設定

1. 務必安裝安全通訊端憑證(SSL)。
2. 建議主機上安裝相關防護機制，如端點偵測回應(EDR)、託管偵測回應(MDR)。
3. 移除 WebITR 所使用上傳資料夾之執行權限。
4. 系統之最高權限帳號(administrator/root 及資料庫的 sa 帳號)應僅供 WebITR 安裝機關主機管理者使用，不可提供其他使用者、維護廠商或系統程式使用。
5. 落實人機帳號分離，且不可多人共用帳號。
6. 所有主機帳號之權限應以最小化為原則，僅提供必要之權限；所有主機密碼皆需符合最小長度、複雜度、定期變更等密碼原則。
7. 應定期審核帳號權限妥適性及帳號留存必要性，不需使用或久未啟用之帳號應移除。
8. WebITR 應用程式應與其資料庫使用不同主機，且資料庫主機應放置於內網，並於防火牆規則設置僅開放應用程式主機連線。
9. 建議 WebITR 應用程式與資料庫之主機採用異機或異地備份。

（三）WebITR 系統設定

1. WebITR 安裝機關於接獲 WebITR 維護廠商通知有新版本時，應儘速完成版本更新，或加入本總處自動版更作業。
2. 機關設定之登入系統方式為帳號密碼者，應於登入頁面啟用驗證碼機制。

3. 應依密碼安全設定原則設定相關參數（包括密碼長度、複雜度及更新頻率），以確保使用者之密碼強度。

4. WebITR 安裝機關若有發現任何 WebITR 資安漏洞或弱點，應立即提供相關資訊供本總處修正。

四、 WebITR 使用機關應行注意事項

（一）應管控使用者將個人連網設備(例如個人手機)連接其辦公電腦之行為，以避免其個人連網設備遭駭客或有心人士作為跳板進行內部攻擊或舞弊行為。

（二）使用機關應定期審核帳號權限妥適性及帳號留存必要性，不需使用或久未啟用之帳號應移除。

（三）使用者應配合系統設定定期更新密碼，且不可將帳號及密碼提供他人知悉或隨手記載於容易被窺視之處。