中國建設銀行企業金融網路銀行使用安全須知

中國建設銀行台北分行提供之企業金融網路銀行之安全機制完全遵循最新、最高安全水準之國際標準及業界技術規範，亦符合當地主管機關的標準，您當可安心使用本行所提供的網路銀行各項服務。

依據分析目前所發生的網路交易安全問題，大多數是出自人為操作上的疏忽，只要平常稍加注意，就不會發生任何的損失！

為此，我們特別提供下列安全須知供您參考，並提醒您應時時注意：

一、妥善保管登入代號與密碼

※ 登入代號、密碼與動態密碼機 OPT 應分開保管。

※ 不要使用易被破解之數字做為密碼（例如：統一編號、個人身份證號碼、生日、電話或重複的數字）。

※ 當您申請相關業務時，請於第一時間內變更銀行寄送給您的密碼函內之密碼，並牢記。

※ 請您經常不定期變更您的各種密碼。（尤其懷疑密碼有外洩情形時更應馬上變更）。

※ 切勿將個人的任何密碼告知他人。

※ 請勿將任何密碼書寫於明顯且易讓他人取得之處。

※ 輸入密碼時注意不要被周遭他人窺視。

※ 若您的動態密碼機 OPT 遺失時，請立刻向本行申請掛失，以避免遭他人盜用影響您的權益。

※ 當您使用的密碼已連續錯誤了 5 次，本行將暫停該密碼對應的網路銀行功能，若欲恢復相關功能或您懷疑有不法人士以嘗試錯誤方式猜測密碼時，請立即洽客戶服務專線由本行專責人員協助處理。

二、確認登入正確的網址

本行企業網路銀行之網址如下列：

https://Intl.ccb.com/

若非本行合法註冊的企業網路銀行網站，請勿輸入任何本行客戶代號、使用者代號及密碼，以避免遭偽冒之網站騙取您的登入資料。

三、交易完畢或臨時離座時請一定要簽出網路銀行並關閉瀏覽器

當您因故臨時離座或執行完所有交易或查詢動作之後，記得一定要簽出網路銀行，並關閉瀏覽器，以避免旁人利用瀏覽器之相關功能取得您交易或

查詢的重要資料。

四、盡量不要使用公共場所提供的電腦進行網路銀行交易

請盡量不要使用公共場所提供的電腦進行網路銀行交易，以避免暫存在電腦內登入之統一編號、使用者代號及密碼及所有交易記錄等資料，被有心人士所截取。

五、定期更新您電腦上的防毒軟體版本並掃除病毒

有心人士可透過病毒或類似之惡意程式碼(如特洛依病毒)取得您存於電腦內的相關資料，請在您的電腦上安裝防毒軟體，並定期更新病毒碼版本，同時掃除病毒。

六、避免開啟未知來源的 Email，避免從可疑網站下載軟體

請不要透過 Email 內之連結、網路搜尋引擎、可疑跳窗網站或其它可疑通路登入網路銀行，請於瀏覽器網址列直接輸入認證過網址或將網站加入我的最愛於登入直接點擊，如果您發現可疑網站，請立刻與本行聯絡。

七、定期檢視交易紀錄

定期檢視交易紀錄,如果發現帳戶有任何可疑交易,請立即向銀行回報。

感謝您使用中國建設銀行企業金融網路銀行所提供的服務，希望以上的提醒能協助您更安全地運用網路銀行所帶來的便利，若對本行網路銀行使用上有任何安全疑慮，請聯絡您的客戶經理為您作詳盡之解說。