电子银行安全提示

为了保障您的账户安全，我们提供各项保安措施并安排系统定期升级，也建议您采取以下各项保障网上活动的措施：

确保移动装置的安全及版本更新（适用于手机银行）

- 小心保管您的手提电话和 UKey。 如 UKey 遗失，请立即联系我们更换 UKey。
- 只下载民生香港提供的官方应用程序和更新。 请于 Apple App Store / Google Play Store 下载安装或于官方网站 www.cmbc.com.hk 直接下载。请不要在其他途径下载中国民生香港分行企业手机银行应用程序，尤其是经可疑 QR Code 下载。
- 使用可靠的无线网络或工具，及确保其安全性。
- 为减低风险，建议使用时移动银行时关闭移动装置上的无线支付功能，如支付应用程序及 NFC 功能等。

确保使用安全的计算机及浏览器（适用于网上银行）

- 客户如需使用网上银行服务，应确保使用正确网址登入。您可在浏览器上网站地址一栏直接输入银行正确网址 www.cmbc.com.hk 进入网上银行服务，切勿经含有连结的邮件、网上搜寻工具或可疑弹出窗口登入。注意本行不会透过邮件向客户发出含有嵌入式连结至网上银行服务的内容。
- 请您安装防火墙程序及定期更新病毒检测软件，以预防新病毒的入侵。
- 您应取消浏览器的“自动完成”功能，以避免当您键入密码时，计算机会自动完成您的输入。要启动或取消“自动完成”功能，请打开浏览器，选择“工具”-“Internet 选项”—“内容”—“自动完成设置”，取消“表单上的用户名称和密码”功能。

使用安全的用户别名和密码

- 为提高安全，我们强烈建议您的登录密码和 UKey 密码均采用 6 位或以上的组合，应选用一个别人不会容易猜到的密码，并包含数字、字母及混合大小写，例如：Ci27Ld98。
- 请紧记您的用户别名和密码切勿用笔写下。切记时刻妥为保密这些资料，切勿向任何人(包括本行职员及警方)透露。

- 定期更改您的密码，建议每 60 天更改一次。
- 当您在登入时，请确定没有人在背后或附近察看，与及确定其他人不能透过手机屏幕看见您所输入的用户别名及密码。
- 请不要在非民生银行官方网站或其他非法网站上输入公司的银行账号及密码等信息。

正确地登入/ 登出

- 建议以 UKey 登入。如以用户别名进行登录的用户，建议用户别名使用不会轻易被人猜中的组合， 避免和密码重复使用。
- 如果您输入不正确的 UKey 密码且超过 6 次，您的 UKey 将被停用，需向我们重新申请新 UKey。
- 如果您在同一天内输入不正确的登录密码且超过 5 次，当天不可再登入。登入次数为网银和手机银行共享。
- 在您每次登入时，我们会提供您的别名、上次登入渠道、时间和当日登入次数等信息。如果您怀疑有任何不寻常的活动或对最近一次登录时间及本日累计登录次数等有疑问，请立刻更改登录密码并致电客户服务热线。
- 建议您选择在每次登录时收取短信通知，了解登录信息。
- 若在指定时间内没有任何活动，网上银行/手机银行服务将自动注销，再次使用需重新登录。
- 谨记网上银行使用完毕后，请选择安全退出，并及时拔下 UKey。

安全操作交易及定期检阅账户

- 切勿透过安装在公众地方的电脑（例如网吧等）进行任何交易。
- 进行授权交易时，您必须仔细核对收款人的身份和账户数据，与 UKey 屏幕上的信息是否吻合，才输入 UKey 密码。
- 留意有关确认交易的手机短讯，并核对事务数据。
- 为及时收取短讯，如流动电话号码有所更改，客户须尽快于网上银行更新或通知本行以作出更新。
- 定期查阅您的户口结余及结单，以检查有没有异常的账项。
- 发现账户有未经授权交易，或账户有任何不寻常活动，请实时联络我们。