恒生銀行
HANG SENG BANK

电子管道安全性措施

本文件将说明电子银行业务系统 (下称「**电子管道**」) 的安全性措施 (恒生银行或HSBC集团可能会不定期修订或更新)，适用范围为恒生银行或HSBC集团旗下任何成员(下称「**银行**」) 向客户 (下称「**客户**」) 提供的任何电子银行业务系统。

银行安全性措施

1. 银行应采取相关措施，拒绝未经授权的外部人士存取其网际网路服务营运的环境。
2. 银行应确保自家系统受到严格控管，包括设立营运持续方案。
3. 根据银行的安全性措施，由客户授权存取恒生 HSBCnet 电子管道的使用者 (下称「使用者」) 若长达 6 个月未有登入恒生 HSBCnet，可能会自动被系统暂停使用。如有恒生 HSBCnet 之设定档在长达 18 个月的时间中没有任何使用者户存取，该恒生 HSBCnet 设定档可能也会被暂停使用。
4. 如果使用生物特征验证方式 (如指纹扫描或脸部辨识) 从行动装置存取电子管道，银行及其提供应用程式至行动装置的关联 HSBC 实体，保留任何时间视需要移除生物特征验证功能的权力，若装置有安全性相关疑虑则不另行通知。在正常情况下，仍然可以使用其他现有方法透过行动装置进行验证。

客户安全性措施

1. 客户只能透过银行指定的验证方式存取电子管道。
2. 客户应确保所有使用者均能妥善保管其安全性认证 (密码、提示问题的答案、安全性答案、安全装置 PIN、行动装置密码 / PIN 或任何需要存取电子管道的安全性认证 (如适用)) ，并维持此类资讯的机密性，同时不帮助对这些认证进行任何未经授权的使用。
   特别是客户不得与任何第三方分享任何安全性认证或存取电子管道，但已获得客户授权且受到规范之第三方服务供应商则不在此限。
3. 客户有责任谨慎挑选使用者，须考量到这些使用者将能存取多种功能，包括向账户或其他服务指派权限，以及传送与这些账户或服务有关的指示。
4. 若任何安全装置遗失或遭窃，客户应立即通知银行。
5. 客户应：
   (a) 在怀疑任何使用者的认证透过任何方式遭到部分或完全盗用时，立即采取适当动作保护该使用者的设定档；
   (b) 在怀疑任何使用者的认证遭盗用时，审查其账户和使用者设定档的近期活动，并在有任何异常情况时，立即通知银行；以及
   (c) 定期审查其账户和使用者设定档的活动，借此确保没有违规行为，并在有任何异常情况时，立即通报银行。
6. 如有任何使用者离开客户的机构，客户应立即从电子管道设定档中移除该使用者。若对使用者的行为或权限有任何疑虑，客户应立即暂停该使用者对电子管道的使用。客户应确保安全性认证或装置仅由指派的特定个人使用者使用，但已获得客户授权且受到规范之第三方服务供应商则不在此限。
7. 客户应确保其使用者在银行提出要求时，皆提供正确，详实且未经省略的详细资料。客户应进一步确保其使用者会定期检视此类资讯，并在有所变更时更新详细资料，且任何时候皆只维护一个使用者名称或一组安全性认证。
8. 客户若得知银行已寄送安全装置，却未收到寄送的包裹，则应在寄送后的七天内通知银行。
9. 若經銀行要求，客戶應立即將任何安全裝置歸還給銀行。
10. 客户应定期采用及审查其内部安全性措施，借此确保所有保护措施保持在最新状态，并符合法规及产业的最佳实务指示。这包括但不限於恶意软体防护、网络限制、实体存取限制，远端存取限制、电脑安全性设定、不当使用情况的监控、可接受的网路浏览器与电子邮件使用方式(包括如何避免收取恶意软体) 的指引。
11. 客户应设立相关流程，避免使用者遭受到社会工程攻击或听从诈骗通讯的指示行动。这是为了防止企业电子邮件遭盗用和其他类似的攻击手法，避免诈骗者冒充为电子管道之授权使用者已知的对象，并寄送电子邮件给授权使用者，企图变更收款对象的地址或银行账号。此类流程应包括如使用者收到看似来自已知寄件者(包括但不限於高级管理阶层、供应商和厂商) 的通讯内容时，如何确保独立验证 (透过电子邮件以外的方式) 此类通讯内容的真实性。
12. 若使用者透过行动装置存取任何电子管道，客户应要求该使用者：
    (a) 登入任何电子管道后，切勿让行动装置处於无人看管的情况下；
    (b) 存取完任何电子管道后，按「登出」按钮；
    (c) 启用行动装置的自动密码锁定功能；
    (d) 不与他人共用用于存取电子管道的行动装置;
    (e) 为装置中唯一注册了生物验证 (脸部辨识、指纹、声音、视网膜) 的人；
    (f) 於发生第 15 条假设情境之场合，采取行动以取消注册不得再度用于验证的装置；以及
    (g) 不使用任何已越狱，取得根权限或遭破解的行动装置存取电子管道。
13. 客户瞭解并同意，其电子管道若因任何原因遭停用，该电子管理后续的任何重新启用作业，都会将所有权限、限制、使用者存取权以及对相同账户和服务的存取权，恢复至停用前的原始状态。
14. 客户应瞭解，使用行动装置存取电子管理的使用者可以透过该装置执行广泛的活动。这包括使用行动装置 (如代替安全装置) 验证经由桌上型电脑在另一电子管道执行的活动。
15. 当使用者经由某些行动装置上可用的生物特征验证方式存取电子管道时 (如指纹扫描或脸部辨识) ，客户瞭解此种验证方式依旧存在遭破解或允许未经授权的存取的风险 (例如亲近的家庭成员涉入) 。