恒生銀行
HANG SENG BANK

# 恒生HSBCnet安全特点

# 恒生银行的网上安全方针

本行旨在为客户提供稳健、可靠且安全的线上业务环境。 我们设法透过采用「同类最佳」的技术、制定最佳实务资讯科技政策及程序的组合，并让专业资源致力於实行及监督，以达成我们的目标。 我们采用业界标準解决方案，在客户登入时验证其身分，确保以安全可靠的方式传输客户资料，并保护客户资料的安全。我们拥有备分及应变计划，可确保将不论因为任何原因而发生服务中断状况的机率降到最低。凭借我们作为安全电子银行业务系统提供者，拥有丰富经验，我们还运营一个控制及支援结构，旨在确保银行在提供网上银行交易时，能因应所面临的各种风险层面。

## 安全特点

- 稳健身份验证流程
- 防止键盘记录及阻断服务攻击
- 使用实体保安编码器或流动保安编码器产生的一次性密码进行双重验证
- 采用「传输层安全性」(TLS) 加密技术保护客户与恒生银行之间的资料传送
- 保护敏感资料传送及储存确保客户资料机密性
- 采用业界标準的安全机制保护基础建设
- 定期对系统安全进行独立审查
- 涵盖系统及安装开发与管理的稳健且定期审查的资讯安全政策
- 全面的应急及后备安排
- 24/7 安全监控及中央事故管理团队
- 行政及交易活动的审计追踪

# 恒生HSBCnet验证

## 安全认证及双重验证

恒生HSBCnet旨在根据一系列认证，来验证登入系统的使用者。每一种认证都经过设计，能对抗我们在网际网路上验证身分时面临的多种风险。恒生HSBCnet 会设法以多种方式验证使用者的身分，每种方法都经过特别设计，会将被存取的服务或功能的相关风险，与适当的安全级别进行比对。这些方式包括传统的使用者名称及密码，并使用「提示问题」的额外认证加以辅助，加强针对阻断服务攻击的保护，以及使用实体保安编码器或流动保安编码器产生的一次性密码进行双重身份验证。

风险较高的服务及功能受到双重身份验证的保护（在以实体保安编码器及流动保安编码器登入级别的情况下）。双重验证是传统密码式安全性防护的加强版，因为它不仅基於阁下已知的资料（在本例中为使用者名称及实体保安编码器或流动保安编码器的密码），阁下亦必须拥有实际的工具（即已启动流动保安编码器的流动装置或实体保安编码器），以及阁下固有的东西（即已於流动装置启用的生物认证（Touch ID / Face ID / 指纹认证 – 如启用）。因此，潜在的攻击者必须取得第二个或第三个因素 (即实体保安编码器或已启动流动保安编码器的流动装置及其密码或生物认证)，才能入侵使用者的帐户，因此这种验证方式可以消除因网际网路上分散所导致的诸多渗透风险。

## 未经授权的存取尝试

若有人试图存取阁下的恒生HSBCnet帐户，却无适当的认证，系统将会在数次不成功的尝试后锁定帐户。但是，为了降低他人恶意锁定阁下的恒生HSBCnet帐户的风险，本行也实施了阻断服务攻击防护。目的是确保只知道使用者名称的人士受到质疑时，无法借由输入错误数值而锁定该使用者的帐户。

## 使用TLS已加密的工作阶段

在阁下输入安全性敏感资料(例如：密码)时，画面上会遮蔽这些字符。当资料从客户的浏览器传送到恒生银行时，系统会将传送的资料加密(透过TLS，亦即「传输层安全性」)。抵达恒生银行时，此资料会在数据库内加密。即使恒生HSBCnet的系统管理员也无法存取这项资讯。

若有人取得我的认证且能存取系统，我要如何判断是否发生过这种情况?

恒生HSBCnet应用程式内有客户可以使用的工具，用以检阅特定使用者执行过的活动。

- ❖ 当阁下登入时，阁下的主要登陆页面会指出此帐户上次登入的时间。
- ❖ 使用者帐户执行的任何业务或管理活动，都能借由「活动查询」工具检视。

## 资料传输安全

阁下与恒生HSBCnet之间的安全性详细资料传输，以及所有线上管理或交易活动，均使用TLS通讯协议加密。

基本加密涉及从一方传输资料到另一方的过程。传送方会将资料编码后再传送。接收方必须以正确的「解码器」将资料解密后才能读取及使用。加密的效果是以使用的密钥的复杂程度来衡量的。密钥越复杂，没有正确解码器的人破解程序代码的时间则越长。

TLS是一种业界标准协议，用于保护网络浏览器与恒生银行之间的互联网通讯。恒生银行目前支援TLS 1.2及以上版本。

## 资料机密与完整性

恒生银行采用安全行业最佳实务来保护客户或个人资料。注册时，每个使用者都会看到银行的资料隐私声明，声明中详述我们为使用者提供的保障并寻求使用者的同意。此外，使用者的资讯不会被写入软盘，或储存在与网际网络链接的网路服务器上。网路服务器实际上与保留传输资料的后台数据库是分开的。因此，我们不会在网络服务器上保存客户交易资料。敏感资料，例如客户密码，则使用硬件安全模块储存在加密数据库中。

# 恒生HSBCnet功能特点

以下描述恒生 HSBCnet 内建的一些功能特性，让阁下更轻松地控制系统的使用。

## 存取级别

恒生HSBCnet为客户员工提供两种存取级别。系统管理员可以执行(在双重或单方控制下)一般管理工作，例如设定及授权使用者使用恒生HSBCnet 的工具，以及暂停或删除使用者。

终端使用者无权存取管理功能。任一类型的使用者都能被分配交易功能，但系统有足够弹性，因此可以完全隔离管理与交易功能。

## 使用者存取控制

存取控制工具允许阁下指定的恒生HSBCnet系统管理员决定个别使用者的存取权利及权限，以及帐户级别检视及付款授权限制。

阁下可以设定授权付款所需的使用者人数，以及不同付款金额的使用者级别组合。阁下可以建立一套系统，要求不同国家或总公司对超过特定金额的付款进行授权。这可完全控管存取及授权，同时提高付款处理效率。

## 双重授权管控

恒生 HSBCnet 中的所有重大的管理及业务功能均能以双重授权控制（一名使用者提交交易/请求；另一名则需要为其授权）。 然而，应用程式也为客户提供灵活性，让他们可以定义是否需要双重授权）。但是，在正常操作情况下，我们强烈建议选择双重管控选项。

## 活动记录工具（审计追踪）

主要管理及交易事件会由恒生HSBCnet记录，并提供使用者透过活动查询记录工具在线上检视。我们会提供审计追踪，允许追溯内部控制及系统活动的财务审查。

## 逾时操作

恒生HSBCnet会强制执行閒置（无活动）的逾时操作。若操作时段在一段时间后维持无活动，操作时段会被终止，使用者必须重新登入应用程式。此外，使用者在操作时段期间检视的页面，在逾时后也不会储存在浏览器中，让其他使用者稍后可以存取这些页面。

# 恒生HSBCnet安全性準则

阁下需为自己的系统，连接，以及提供给银行的指示负责。阁下必须实施下列措施以保护自己，包括：

## 安全凭证

使用者必须随时保管好自己的安全凭证（密码，提示问题答案，实体保安编码器或流动保安编码器的密码，或其他存取恒生HSBCnet所需的安全性凭证），并确保没有未经授权使用或试图入侵这些凭证的情况。尤其是：

- 切勿写下，记录或向其他人泄露这些凭证;
- 立即销毁任何来自银行或其他方的凭证通知;
- 请勿使用容易猜到或推断的安全凭证（例如：个人详细资料，简单的数字组合);
- 切勿在任何可自动保留凭证的软件上记录密码，提示问题答案，安全性答案，或保安密码(例如：电脑萤幕提示或使用者网际网路浏览器的「储存密码」功能);
- 确保使用者在登入恒生HSBCnet时并无受到任何人士偷窥或闭路电视的监视；
- 强烈建议使用者拥有仅用于存取恒生HSBCnet 的专属终端机，以降低恶意程序代码被加载到装置的可能性。此装置不应用于一般的网页浏览、电子邮件或社交网络；
- 切勿向阁下的任何员工或组织内部透露任何安全凭证。 阁下应谨慎留意任何声称来自银行或任何第三方要求披露任何密码、使用者安全凭证或任何帐户详细资料的信件或通讯。 一旦发生此事，阁下必须尽快向银行在发生任何可疑活动、任何顾虑或可疑信件或通讯时立即向银行报告；
- 请确保，倘若阁下怀疑凭证以任何方式遭到全部或部分洩漏，请立即采取妥善行动，借由变更凭证或在采取妥善行动时暂停使用者，以保护其使用者的设定档。一旦阁下怀疑任何凭证已被洩漏时，也应尽快检查其银行帐户最近的活动以及使用者设定档，借此识别任何未经授权的行为；且
- 阁下有责任定期审查其银行帐户及使用者设定档活动，以确保不存在任何违规行为，倘若发现任何违规行为，阁下必须立即通知银行。

## 系统相容性

阁下必须确保拥有兼容的硬体及软体以便存取相关的恒生HSBCnet。恒生HSBCnet客户指南中详列了最低系统需求。
阁下同意操作资讯技术及系统控制项目时遵守相关法律及规定，例如沙宾法案(Sarbanes–Oxley)。

## 安全标準

阁下必须定期审查其内部安全措施，借此确保所有保护措施保持在最新状态，并符合法规及业界最佳实践指南。尤其包括但不限於：

- 阁下使用与恒生HSBCnet相关的加密技术必须符合使用者存取恒生HSBCnet所在地的当地法律;
- 阁下应使用并维护垃圾邮件过滤器，桌面防火墙，以及即时防毒软件。收到更新时，必须在相应的时间间隔内更新这些工具，并用来扫描阁下的电脑;
- 阁下应在操作系统及所有应用程式的安全性更新及应用程式修补程式推出时，立即更新且安装；
- 切勿使用公共网际网路存取点(例如网吧，公共Wi-Fi热点）来存取恒生HSBCnet或阁下的帐户或个人资讯。若必须使用这些存取点，则请务必采用VPN (虚拟专用网络)。

# 恒生HSBCnet 存取

为防止未经授权存取恒生 HSBCnet 及 / 或降低阁下遭受任何潜在安全威胁的风险，阁下必须确保：

a) 使用者在使用后登出恒生HSBCnet，并在登入恒生HSBCnet时不允许存取这些终端机；
b) 使用者要按照指定的登出流程（在恒生HSBCnet内，使用者应选择萤幕右上角的「登出」按钮），正确登出恒生HSBCnet，而非仅仅关闭浏览器视窗；以及
c) 尚未确认来电者身份前，阁下切勿在电话中提供任何资讯。 阁下有责任透过独立方式，亦即联系公开线路或已知联系人，联络银行蒐集资料，并确认来电者的身份。银行绝不会要求阁下提供任何密码资讯。

若有任何未经授权，或可疑的存取或使用恒生 HSBCnet（包括凭证），或任何未经授权、未知或可疑的交易、通讯或指令发生，阁下必须立即通知银行。
若阁下遇到下列情况时必须立即通知银行：

- 其存取恒生 HSBCnet 的浏览器出现异常及 / 或无回应；
- 发现内容显示方式有变化;
- 收到银行提供的安全凭证后，又收到讯息表示系统无法使用;
- 在操作时段期间，收到未预期的讯息，要求提供安全凭证或电子簽章；
- 收到不寻常的弹出讯息； 或
- 发现新的或未预期的工具列及 / 或图示

若阁下发现可疑活动，必须立即停止在恒生 HSBCnet 的所有线上活动，并从网络中删除任何可能受到入侵的电脑系统。

当使用具备簽署功能的安全装置执行电子簽署时，使用者必须核实系统要求其簽名的资料正确无误（亦即系统要求他们透过恒生 HSBCnet 簽署的受款人帐号，与内部付款系统或文件上的资料一致）。若发现网上提供的资讯与实际活动详情有出入，阁下必须立即通知银行。

使用者在使用恒生 HSBCnet 及 / 或任何可以透过恒生 HSBCnet存取的产品或工具时，有任何实际或可疑的不当情况，或使用者已无权使用恒生 HSBCnet（由于离职或其他原因）时，阁下必须立即移除其使用者的存取权限，并立即通知银行。

为了找出实际或潜在安全性违规事件，阁下必须遵守银行、警方或其他监管机构所提出的合理要求。 阁下必须对透过恒生 HSBCnet，每日执行款项对帐的指示。

## 暂停使用者

恒生 HSBCnet 允许系统管理员暂停其他使用者的帐户。 此功能仅限於需要令使用者暂时无法使用恒生 HSBCnet 的情况下使用，例如放假。此功能的目的不是於使用者行为存有重大安全疑虑时使用。 在此情况下，系统管理员应立即从恒生 HSBCnet 删除该使用者的帐户，并撤销该使用者的实体保安编码器（如持有）或流动保安编码器。

若暂停是唯一可用的选项（例如：因为必须紧急停用该使用者，且没有其他系统管理员可以批核删除指示），则应与其他保护措施一并执行（例如：取回使用者的实体保安编码器（如持有））。 如有疑问，请致电银行寻求协助。 使用者需要处於「启用中」或「已批核」的状态下才能被暂停。 一旦使用者被暂停，於重新启用或删除前，切勿对该使用者的帐户或存取权限进行任何维护。

# 恒生HSBCnet 流动理财服务

除了遵守一般电子管道安全性措施的义务外，阁下还必须确保遵守与流动装置上的恒生 HSBCnet 流动理财应用程式相关的附加安全要求**，包括:

- 不要在流动装置上储存阁下的恒生 HSBCnet登入或个人资料。
- 使用流动装置连接到无线网络时，仅使用受信任的网络或服务供应商，并启用额外的安全保护，例如Wi-Fi Protected Access (WPA)。
- 旅行时，尽可能使用可靠的电脑或流动装置。确保阁下的装置已安装最新的制造商软件更新，并避免使用「已越狱」的装置，或「已取得 root 权限」并未经授权修改的装置。
- 请勿与他人共用流动装置。为防止他人盗用装置，请启用密码 / PIN 码锁定功能。
- 使用安全性强，且黑客无法轻易猜测或推断的 PIN 码，并定期更改 PIN 码。阁下可以随时在恒生 HSBCnet流动理财应用程式设置中更新阁下的HSBCnet保安密码。
- 登入恒生 HSBCnet流动理财应用程式后，请不要离开或閒置阁下的流动装置。当使用完后，请确保阁下已完全登出恒生 HSBCnet流动理财服务及关闭程式。
- 不要在阁下的流动装置上安装来源不明的应用程式。

** 有关阁下使用恒生HSBCnet流动理财应用程式的安全义务的完整详情， 请参阅「**电子管道安全性措施**」。