外部第三方供应商个人信息保护政策

本版本更新日期：2026 年 5 月 9 日
生效日期：2026 年 5 月 9 日

Note: English Language China Privacy Notice also included in this document, see page 15

本个人信息保护政策（“**本政策**”）适用于外部第三方供应商(“**供应商**”或“**贵公司**”)在为附件一所列的汇丰集团在中国内地的实体（“**汇丰**”或“**我们**”）提供服务过程中所涉及的供应商相关个人信息。我们将根据本政策处理贵公司相关个人信息主体(“**关联个人**” 或“**个人信息主体**”)的个人信息。为本政策之目的，关联个人或个人信息主体指任何与贵公司有关系的人士，包括但不限于任何公司董事、监事或职员、合伙组织的合伙人或合伙成员，股东、主要拥有人、控制人、指定账户持有人、指定收款人、贵公司的代表、代理或指定人士、或其他在贵公司和汇丰集团之间的关系中有关联的其他个人。

请贵公司在向我们提供个人信息前仔细阅读本政策，并请确保相关个人信息主体知悉本政策，并应特别告知该人士我们将如何处理其个人信息，并取得该等人士的有关授权同意。贵公司可提醒该人士事先阅读本政策，也可以向该人士提供本政策的副本。

注意：若贵公司不同意本政策的相关条款，请勿提交贵公司的个人信息。对本政策中我们认为与贵公司和/或关联个人的权益存在重大关系的条款和/或涉及敏感个人信息处理的条款，我们采用粗体字加下划线进行标注以提示贵公司特别注意。

个人信息保护政策概述

我们深知个人信息保护的重要性，会尽力保护贵公司的关联个人信息安全。我们致力于维护贵公司对我们的信任，恪守以下原则保护贵公司的关联个人信息：权责一致原则、目的明确原则、选择同意原则、最小必要原则、确保安全原则、主体参与原则、公开透明原则等。同时，我们承诺依法采取相应的安全保护措施来保护贵公司的关联个人信息。

本政策包括以下内容：

一、 我们如何保护贵公司的关联个人信息

1. 信息安全是我们的首要关切。我们在任何时候竭力保障贵公司的关联个人信息不被擅自或意外取得、处理或毁损。我们采取各种合适的安全技术和安全管理等措施保护贵公司的关联个人信息，以实现我们对信息安全的承诺。如果由于我们的原因导致贵公司的关联个人信息被非授权访问、公开披露、篡改或毁坏，导致贵公司和/或关联个人的合法权益受损，我们将依法承担相应的法律责任。

2. 我们的网站支持先进的内容加密技术保护贵公司的关联个人信息。这种加密技术是目前互联网上保护数据安全的行业标准。当贵公司通过我们的网站、应用程序提供敏感个人信息时，这些信息会被自动加密，以便后续安全传输。我们的网站服务器装有防火墙，并且我们的系统处于监控之下，以防未经授权的访问。

3. 我们设有严格的安全系统，以防止未经授权的任何人获取贵公司的关联个人信息。我们对可能接触到贵公司关联个人信息的员工采取了严格管理，包括但不限于对不同岗位采取不同的权限控制，与相关员工约定保密义务，制定、实施有关信息保密与安全的规章制度并提供相关培训。

4. 除非是为了遵守法律法规或监管规定，根据本政策、相应的另行约定（如有）或基于贵公司/关联个人的另行单独同意或授权行事，我们不会向任何第三方披露贵公司的关联个人信息。当我们需要使用外部服务机构/人士提供的服务时，我们也会与其约定严格的保密义务，要求他们对贵公司的信息采取保护措施并严格遵守适用的法律法规要求来处理贵公司关联个人信息。

5. **对于贵公司的关联个人信息安全，贵公司与我们同样负有重要责任。贵公司应妥善保管贵公司的关联个人信息，包括与之相关或可能记录该等信息的文件、设备或其他介质，并应只在安全的环境中使用该等信息及相关文件、设备或其他介质。在任何时候，贵公司均不应向任何他人透露或允许任何他人使用该等信息或相关文件、设备或其他介质。如贵公司认为贵公司的关联个人信息及/或相关文件、设备或其他介质已经泄露、遗失或被窃，或发生其他可能影响信息安全的情形，贵公司应立即通知我们以便采取适当措施防止损失扩大。**

6. 我们会定期组织内部相关人员进行应急响应培训和应急演练，使其掌握岗位职责和应急处置策略和规程。若不幸发生个人信息安全事件，我们会启动应急预案，采取相应的处置和补救措施，防止事件升级、损失扩大。同时，我们将按照法律法规的要求向贵公司告知：安全事件的基本情况和可能的影响、我们已采取或将要采取的处置措施、贵公司可自主防范和降低风险的建议、适用的补救措施等。我们将及时将事件相关情况以邮件、信函、电话、短信、推送通知或其他合适的方式告知贵公司。难以逐一告知供应商时，我们会采取合理、有效的方式发布公告。请贵公司及时将相关情况根据法律法规的要求告知相应受影响的关联个人。同时，我们还将按照法律法规以及权力机关的要求，向权力机关报告个人信息安全事件及其处置情况。

二、 我们如何收集贵公司的关联个人信息

1. 个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息包括姓名、出生日期、身份证件信息（身份证、护照等）、个人生物识别信息、通信通讯联系方式、住址、账户信息、财产状况、位置信息等。

敏感个人信息是指一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、人格尊严、身心健康受到损害或歧视性待遇等的人身及财产信息，主要包括：身份证件信息（身份证、护照等）、个人生物识别信息、财产信息、交易信息、健康生理信息、特定身份、金融账户、行踪轨迹等信息以及不满十四周岁未成年人（即儿童）的个人信息等。

2. 我们可能需要收集的个人信息：

a) 当贵公司申请成为我们的供应商时，我们可能需要收集贵公司的下述关联个人信息：

目的或功能	我们可能需要收集的个人信息
在供应商引入阶段，与贵公司进行联络、沟通；评估，管理供应商申请，开展供应商尽职调查	(1) 供应商法定代表人的姓名； (2) 供应商联系人的姓名、联系方式（包括固定电话号码、手机号码、电子邮箱）和当前职位； (3) 当采购的服务本身经过内部的内在风险评估审查后，合规风险审查评级是高或者非常高，我们需要进一步收集以下个人的姓名、出生日期、性别、国籍和**身份证件信息（包括证件类型、号码）**： • 贵公司拥有超过或等于 10% 股权、投票权或财产（包括不记名股票、资本和利润）的最终实益所有人（自然人）； • 贵公司的所有高级管理人员和执行董事。

b) 当贵公司成为我们供应商后，我们会将上述供应商申请过程中已获取的个人信息进一步用于管理贵公司与我们之间的相关协议订立和履行之目的，此外我们还可能需要进一步收集贵公司的下述关联个人信息：

目的或功能	我们可能需要收集的个人信息
汇丰和贵公司之间的相关协议的订立、履行	(1) 贵公司派到汇丰提供现场服务的工作人员信息 • 个人姓名、国籍、性别、出生日期，**身份证件信息（包括证件类型、号码、有效期限、签发国家或地区）**； • 如基于所提供服务性质需要，还可能会进一步收集背景调查信息，包括身份验证、工作经历、当前住址证明、**犯罪记录查询（仅在法律允许或要求时适用）、是否有负面的公共媒体信息、信用记录查询（仅当法律允许时且贵公司提供服务的人员过去五年内曾在相关国家/地区居住六个月或以上的情形下适用）**、所需资格/资质证明信息、教育背景信息、**制裁调查信息、是否与政要或国际组织高级管理人员有关及相关信息、确认提供服务的员工是否受到法律或监管限制的信息、本地欺诈记录查询（如有）** (2) 贵公司在履行协议过程中提供的其他工作人员和联系人的信息，包括姓名、联系方式（包括固定电话号码、手机号码、电子邮箱）和当前职位。 (3) 当采购的服务本身经过内部的内在风险评估审查后，合规风险审查评级是高或者非常高，我们需要进一步收集以下个人的姓名、出生日期、性别、国籍和**身份证件信息（包括证件类型、号码）**： • 贵公司拥有超过或等于 10% 股权、投票权或财产（包括不记名股票、资本和利润）的最终实益所有人（自然人）；

	• 贵公司的所有高级管理人员和执行董事。

3. 为本政策所述之目的，我们会接收或留取贵公司或关联个人主动提供的个人信息，或依据法律法规、监管规定或贵公司/关联个人的授权或同意，通过适当方式向汇丰集团成员或其他第三方（包括但不限于信用查询机构、信息服务提供商、相关的权力机关、联系人及其他机构/人士）收集、查询、核实贵公司的关联个人信息。本政策中“汇丰集团”指汇丰控股有限公司及/或任何其关联公司、子公司、联营实体及该等的任何分行及办事处或其中任何一个，“汇丰集团成员”具有相同含义。

4. 我们收集的个人信息可能包括纸质、电子或其他任何形式的信息。

三、 我们如何使用贵公司的关联个人信息

1. 我们会基于下述目的、用途使用贵公司的关联个人信息：

(1) 为实现本政策上述第二条“我们如何收集贵公司的关联个人信息”中和下述第六条“信息处理的特殊情形”所述之目的和功能；
(2) 遵守或执行任何适用规范（“适用规范”指适用于任何汇丰集团成员的法律、法规、条例、规章、判决、裁定、自律守则、指令、制裁制度、法院命令、任何汇丰集团成员与权力机关之间的协议，或权力机关之间达成的适用于我们或汇丰集团成员的协议或条约）或任何权力机关的命令或要求；
(3) 履行我们及汇丰集团的合规责任（包括监管合规、税务合规及在任何适用规范项下或任何权力机关要求的合规责任）或执行我们及汇丰集团为履行合规责任而制定的政策和程序；
(4) 为我们第三方风险管理、业务运营和管理之需，包括但不限于监督和审查汇丰的供应商服务采购流程，全球化运营、系统或产品研发、审计等；
(5) 管理金融犯罪风险，预防或禁止非法或违规活动、控制或降低风险，侦测、调查及预防任何现实、涉嫌或潜在的金融犯罪活动（包括洗钱、恐怖主义融资、贿赂、贪污、逃税、欺诈、逃避经济或贸易制裁，以及规避或违反有关此等事宜的任何适用规范的任何行为或企图）（包括可以为此进一步查询或确认相关个人或实体的身份和状况，他们是否受到制裁制度的约束）；
(6) 如果适用，向贵公司收取任何到期未付的款项；
(7) 行使或维护我们的权利。

2. **本政策前述有关信息收集、使用的内容不影响我们按照贵公司与我们另行特别约定的用途使用贵公司的关联个人信息。**

3. 若我们要将贵公司的关联个人信息用于本政策载明或贵公司与我们另行约定的收集、使用用途以外的其他用途，我们会向贵公司告知该等用途等信息，并在适用的法律法规要求时，我们须在使用前再次征得贵公司的同意。

四、 我们如何存储贵公司的关联个人信息

由于我们使用全球采购、应付账款和风险管理系统，这意味着，在监管允许和法律适用的情况下，除了中国内地，贵公司的关联个人信息会被转移到和/或存储在境外管辖区，或者受到来自这些管辖区的访问。截至目前，我们的境外受托服务机构名称和联系方式如下：1）汇丰环球

服务（香港）有限公司 （联系方式：hkdpo.enquiry@hsbc.com.hk）；2） 汇丰环球服务（英国）有限公司（联系方式：ico.correspondence@hsbc.com）。 若我们向境外传输贵公司的关联个人信息，我们将遵守适用法律法规关于跨境数据传输的相关要求。无论是在境内或境外处理个人信息，根据适用的个人信息或数据保护法律，贵公司的关联个人信息将受到我们、汇丰集团成员及其员工以及第三方均需遵守的保密及安全规范的保护。

我们遵守关于数据存储的适用法律法规要求并将贵公司的关联个人信息保存至满足信息收集目的、用途所需的最短保存时间。例如：如果与贵公司的签署合约，我们所收集的任何个人信息将自贵公司合约结束之日起保留 30 年。我们制定了数据保留期限政策，根据不同服务场景和不同服务性质，相应确定各项信息类型的具体保存期限。在该政策规定的相应保留期结束后，我们会将相关信息进行销毁、删除或匿名化处理，或者在销毁、删除或匿名化从技术上皆不可能实现的时候，安全地储存贵公司的这些个人信息并且将这些个人信息与其他的数据处理区隔开来。**但我们依据法律法规、监管规定、档案、会计、审计、报告要求，或贵公司与我们之间的特别约定，为向贵公司、监管机构及其他权力机关提供记录查询而需要继续保留的信息除外。**

五、 我们如何委托处理、共享、转让和公开披露贵公司的关联个人信息

1. 委托处理、共享

为本政策前述之目的与用途，在必要且采取相应的保护措施（参见本政策前述第一条“我们如何保护贵公司的关联个人信息”）的前提下，我们会把贵公司的关联个人信息的部分或全部提供、披露给下列接收者（接收者亦可为上述目的和用途，使用、处理及披露该等信息，但需依法或根据我们的要求采取相应的保护措施）：

(1) **汇丰集团成员；**
(2) **汇丰集团的相关承包商、分包商、代理人、服务或产品供应商、许可方、专业顾问或汇丰集团的关联人（包括其雇员、董事、高级职员）；**
(3) **任何我们或汇丰集团成员的监管机构或其他权力机关，或监管机构或其他权力机关指定的机构或人士；**
(4) **经贵公司授权或依法代表贵公司行事的任何人士，例如贵公司的法律顾问、联系人；**
(5) **与我们的业务/资产转让、重组、处置、合并、分立或收购有关的任何一方。**

当适用的法律法规要求时，我们会向贵公司或关联个人告知我们向第三方提供贵公司关联个人信息的有关事项，包括个人信息接收方的身份、联系方式、处理目的、处理方式和个人信息的种类，并取得贵公司或关联个人的单独同意，法律规定不需要取得个人同意的除外。

若涉及跨境个人数据传输，我们还会与接收方签订适当的数据处理协议，在必要的情况下采用国家网信部门届时制定的标准数据保护合同与境外个人信息接收方约定双方有关数据保护的权利和义务，并赋予关联个人作为第三方受益人执行适用法律法规项下关联个人所享有相关个人信息主体的权利，例如关联个人向境外个人信息接收方行使有关权利的方式和程序等。如贵公司或关联个人希望了解前述个人信息出境标准合同的相关内容，可以通过本政策“九、如何联系我们”所列方式向我们索取相关信息。

2. 转让

除非获得贵公司或关联个人的单独同意，我们不会将贵公司的关联个人信息转让给任何公司、组织或个人，**但在涉及我们的任何业务/资产转让、重组、处置、合并、分立、收购时需要转让的除外。在该等情况下，我们会按照适用的法律法规要求向贵公司或关联个人告知个人信息接收方的身份和联系方式，并要求其继续依法保护贵公司的关联个人信息，如果个人信息接收方变更本政策有关个人信息处理目的、处理方式，其应当重新取得贵公司或关联个人的同意。**

3. 公开披露

除非获得贵公司或关联个人的单独同意，我们不会对外公开披露贵公司的关联个人信息，但根据适用法律法规规定、法律程序、诉讼或权力机关的强制性要求我们可能需要公开披露的除外。

六、 信息处理的特殊情形

一般情况下，我们会基于贵公司或关联个人的同意来处理（比如收集、存储、使用、加工、传输、提供、公开）贵公司的关联个人信息。但是，依据相关法律法规的规定，在以下情形中，我们处理贵公司的关联个人信息不必征得贵公司或关联个人的同意：

(1) **为订立、履行关联个人作为一方当事人的合同所必需的；**
(2) **为履行法定职责或者法定义务所必需的；**
(3) **为应对突发公共卫生事件，或者紧急情况下为保护关联个人或其他个人的生命健康和财产安全所必需的；**
(4) **为公共利益实施新闻报道、舆论监督等行为，在合理的范围内处理个人信息；**
(5) **依照适用的法律法规在合理的范围内处理关联个人自行公开或者其他已经合法公开的个人信息的；**
(6) **法律、行政法规规定的其他情形。**

七、 我们如何使用 Cookies 和同类技术

1. 在贵公司/关联个人访问、浏览、使用我们的网站、移动设备应用程序时，网站和/或应用程序会作记录，以分析网站和/或应用程序的访客人数、一般使用模式及贵公司/关联个人使用模式并优化贵公司/关联个人的体验。其中部分资料将通过"Cookies" 及同类技术收集。该技术让我们的网站、应用程序能够识别贵公司/关联个人的装置，并存储贵公司/关联个人使用网站和/或应用程序的资料，以便为贵公司/关联个人提供持续性的服务、使我们的网站和/或应用程序的内容更符合贵公司/关联个人的偏好。我们可以为上述用途取得 Cookies 及同类技术存储的资料。

Cookies 收集的是不记名的统计资料，并不包括姓名、地址、电话及邮箱地址等个人信息。

2. **大多数本地终端的初始设置为同意使用 Cookies。贵公司/关联个人可以根据自己的偏好管理或删除 Cookies。如果贵公司/关联个人想禁用 Cookies，可更改贵公司/关联个人的本地终端的设置，更改后贵公司/关联个人将无法享受 Cookies 可能带来的便利，但不影响贵公**

司/关联个人正常使用本地终端的其他功能。不同本地终端的更改设置各自有所不同，贵公司/关联个人可以通过下述链接了解部分浏览器的 Cookies 设置管理：

- 在 Chrome 中管理 Cookie
- 在 Firefox 中管理 Cookie
- 在 Microsoft Edge 中管理 Cookie
- 在 Safari 中管理 Cookie

八、 贵公司关联个人的个人信息相关权利

1. 贵公司关联个人有权要求我们按照法律法规及本政策的规定，保障其个人信息安全，并要求行使适用的法律法规赋予其的个人信息相关权利。

2. 贵公司关联个人有权向我们查询我们是否持有其个人信息及查阅、复制其个人信息。

3. 贵公司关联个人有权改变其授权同意的范围或撤回其授权，并按本政策“九、如何联系我们”所列方式进行操作。当贵公司关联个人改变授权范围后，我们将不再处理不属于新授权范围内的相应个人信息。但贵公司关联个人撤回同意的决定，不会影响我们此前基于贵公司或关联个人的授权而开展的个人信息处理。

4. **贵公司有权也有义务及时更新贵公司在汇丰的关联个人信息，以确保相关信息是准确和最新的。**贵公司关联个人有权要求我们为贵公司或其自行更新个人信息提供便利，有权要求我们更正任何有关其个人的不准确的信息。

5. 贵公司关联个人有权要求我们根据法律法规、本政策及贵公司与我们之间的约定，删除或以其他方式妥善处理超过保留期的其个人信息。如我们停止运营，我们将及时停止收集贵公司关联个人信息的活动，将停止运营的通知以逐一送达或公告的形式通知贵公司，并对所持有的贵公司的关联个人信息进行删除或匿名化处理，法律法规或监管部门另有规定或者删除个人信息从技术上难以实现的除外。

6. 本政策不会限制贵公司关联个人作为个人信息主体根据适用的法律法规享有的其他权利。

九、 如何联系我们

1. 任何关于查阅、复制、更正、删除个人信息，改变/撤回授权，处理超过保留期的个人信息，或索取本政策文本及了解我们有关个人信息保护的做法的要求，或行使其他适用的法律法规赋予贵公司关联个人的个人信息相关权利的要求，可通过附件一所列的联系方式向我们提出。

2. 为了保障安全，贵公司关联个人可能需要通过贵公司提供书面请求。我们可能会要求贵公司先验证关联个人的身份，然后再处理贵公司关联个人的请求。

3. 我们将在收到贵公司关联个人的要求后最长不超过 15 个工作日或法律法规规定的更短期限（如适用）内予以回复。

4． 对于贵公司关联个人前述有关查阅、更正以及其他处理个人信息的合理要求，我们不会向贵公司或关联个人收取费用。

尽管有上述约定，对非法、违规、无端重复、需要过多技术手段（例如，需要开发信息系统或从根本上改变现行惯例）、给他人合法权益带来风险、超出合理限度或者技术上不切实际的要求，我们可能会予以拒绝。在以下情形中，我们也可能无法响应贵公司关联个人的部分或全部请求：

(1) **与我们履行法律法规规定的义务或金融监管合规义务相关的；**
(2) **与国家安全、国防安全直接相关的；**
(3) **与公共安全、公共卫生、重大公共利益直接相关的；**
(4) **与刑事侦查、起诉、审判和判决执行等直接相关的；**
(5) **有充分证据表明贵公司或关联个人存在主观恶意或滥用权利的；**
(6) **出于维护关联个人或其他个人的生命、财产等重大合法权益但难以获得关联个人本人授权同意的；**
(7) **响应贵公司关联个人的请求将导致贵公司、关联个人或其他个人、组织的合法权益受到严重损害的；**
(8) **涉及商业秘密的。**

5． 贵公司或关联个人有权就我们有关个人信息保护的做法进行监督或提出建议，并就我们或我们员工的任何侵害贵公司的有关个人信息权益的行为提出投诉或依法求偿。

如贵公司或关联个人有任何疑问、投诉、反馈、意见或建议，请通过本政策前述联系方式与我们进行联络。

十、 本政策的制定、生效、更新及其他

1． **我们制定并在汇丰相关供应商管理网站和／或应用程序发布本政策。本政策于发布之日起生效。**本政策可能不时修改、更新，尤其是发生下列重大变化情形时：

(1) 我们的供应商管理模式或第三方工作人员信息管理模式发生重大变化，如处理个人信息的目的、处理的个人信息类型、个人信息的使用方式等；
(2) 我们在所有权结构、组织架构等方面发生重大变化，如业务调整、破产并购等引起的所有者变更等；
(3) 个人信息对外提供、转让或公开披露的主要对象发生变化；
(4) 贵公司关联个人参与个人信息处理方面的权利及其行使方式发生重大变化；
(5) 我们负责处理个人信息的联络方式及投诉渠道发生变化时；
(6) 其他可能对贵公司关联个人的个人信息权益产生重大影响的变化。

我们会在汇丰相关供应商管理网站和／或应用程序通过弹窗提示或公告等方式发布对本政策所做的变更或更新后的政策。本政策的变更不应削减或限制贵公司关联个人作为个人信息主体根据适用的法律法规享有的权利。

2． 如贵公司或关联个人同时是汇丰集团成员的客户，请参阅与客户相关的个人信息保护政策。

3． 我们网站上的一些链接会指向其他公司的网站，该等网站会有其自有的个人信息保护政策，内容可能与本政策不同。使用其他站点时，贵公司需要确保贵公司对他们的个人信息保护政策感到满意。

4． 本政策中英文本如有歧义，概以中文为准。

附件一

汇丰集团在中国内地的实体名单及联系方式

	法人实体名称	联系地址	邮编	联系人	电子邮箱	联系电话
1.	汇丰银行（中国）有限公司	上海浦东新区世纪大道8号上海国金中心汇丰银行大楼	200120	采购部	chn.sourcing@hsbc.com	021-38886325
2.	北京密云汇丰村镇银行有限责任公司	北京市密云区新东路126-1号	101500	采购部	chn.sourcing@hsbc.com	021-38886325
3.	重庆大足汇丰村镇银行有限责任公司	重庆市大足区北环东路1号	402360	采购部	chn.sourcing@hsbc.com	021-38886325
4.	重庆丰都汇丰村镇银行有限责任公司	重庆市丰都县三合镇平都大道东段107号	408200	采购部	chn.sourcing@hsbc.com	021-38886325
5.	重庆荣昌汇丰	重庆市荣昌区昌州	402460	采购部	chn.sourcing@hsbc.com	021-38886325

	村镇银行有限责任公司	街道海棠二支路3、5、7号				
6.	大连普兰店汇丰村镇银行有限责任公司	辽宁省大连市普兰店南山路3号1-2层	116200	采购部	chn.sourcing@hsbc.com	021-38886325
7.	福建永安汇丰村镇银行有限责任公司	福建省永安市燕江中路 1211号1幢	366000	采购部	chn.sourcing@hsbc.com	021-38886325
8.	广东恩平汇丰村镇银行有限责任公司	广东恩平市恩城新平中路 44号	529400	采购部	chn.sourcing@hsbc.com	021-38886325
9.	湖北麻城汇丰村镇银行有限责任公司	湖北省麻城市玉融街56号	438300	采购部	chn.sourcing@hsbc.com	021-38886325
10	湖北随州曾都	湖北省随州市曾都	441300	采购部	chn.sourcing@hsbc.com	021-38886325

	汇丰村镇银行有限责任公司	区烈山大道205号				
11	湖北天门汇丰村镇银行有限责任公司	湖北省天门市天门新城银座帝景湾三号楼	431700	采购部	chn.sourcing@hsbc.com	021-38886325
12	湖南平江汇丰村镇银行有限责任公司	湖南省平江县新城区商业步行街阳光花园阳光华景 101-102、106室	414500	采购部	chn.sourcing@hsbc.com	021-38886325
13	山东荣成汇丰村镇银行有限责任公司	山东荣成成山大道东段198号商业02	264300	采购部	chn.sourcing@hsbc.com	021-38886325
14	汇丰环球客户服务（广东）有限公司	中国广东省广州市天河区天河路381号太古汇2号办公楼四至十七层	510620	采购部	chn.sourcing@hsbc.com	021-38886325

15	汇丰软件开发（广东）有限公司	中国广东省广州市天河区天河路381号太古汇2办公楼22层	510620	采购部	chn.sourcing@hsbc.com	021-38886325
16	汇丰人寿保险有限公司	中国（上海）自由贸易试验区世纪大道8号汇丰银行大楼29楼	200120	采购部	chn.sourcing@hsbc.com	021-38886325
17	汇丰金融科技服务（上海）有限公司	上海市自由贸易试验区临港新片区环湖西一路859-863单号406室	200120	采购部	chn.sourcing@hsbc.com	021-38886325
18	汇丰保险经纪有限公司	北京市顺义区安祥街12号院3号楼2层201室	101300	采购部	chn.sourcing@hsbc.com	021-38886325
19	汇丰企业服务（上海）有限公司	上海市浦东世纪大道8号上海国际金融公司汇丰	200120	采购部	chn.sourcing@hsbc.com	021-38886325

		大厦 35 层				
20	汇丰前海证券有限责任公司	深圳市前海深港合作区南山街道枢纽大街 66 号前海周大福金融大厦（一期）22F2201 单元	518052	采购部	chn.sourcing@hsbc.com	021-38886325
21	北京汇丰公益基金会	北京市朝阳区东三环中路 5 号财富金融中心 18 层	100020	采购部	chn.sourcing@hsbc.com	021-38886325

Personal Information Protection Policy for Third Party Vendor

Date of Update: 9th May2026
Effective Date: 9th May 2026

This Personal Information Protection Policy ("**Policy**") applies to vendor-related personal information of an external third-party vendor ("**Vendor**" or "**Your Company**" or "**you**") in connection with the provision of services to the entities of HSBC Group in Mainland China ("**HSBC**" or "**we**" or "**us**") listed in Annex I. We will process the personal information of Your Company's relevant personal information subject ("**Connected Person**" or "**Personal Information Subject**") in accordance with this Policy. For the purposes of this Policy, a Connected Person or Personal Information Subject means any person who has a relationship with Your Company, including but not limited to any director, supervisor or employee of the company, partner or member of a partnership, shareholder, any substantial owner, controlling person, designated account holder, designated payee, representative, agent or nominee of Your Company, or any other individual who is relevant to Your Company's relationship with the HSBC Group.

Please read this Policy carefully before providing personal information to us, and please ensure that the relevant Personal Information Subject is aware of this Policy and should specifically inform the person how we will handle their personal information and obtain the relevant authorization and consent of such person. Your Company may remind the person to read this Policy in advance, or you may provide the person with a copy of this Policy.

IMPORTANT: Please do not submit Your Company's personal information if Your Company does not consent to the following provisions stated in this Policy. Please pay particular attention to the provisions that are bolded and underlined which we think have material impacts on the rights of Your Company/Connected Persons and/or deal with sensitive personal information of Your Company/Connected Persons.

Personal Information Protection Policy Overview

We fully understand how important personal information is, and we will exert our best effort to protect the security of your Connected Person's information. We have always been committed to maintain your trust and will stick to below principles to protect your Connected Person's information: Right and Responsibility Consistency, Explicit Purpose, Freely Given Consent, Minimum and Necessity, Assurance of Information Security, Participation, Fair and Transparency. We are also committed to take appropriate security measures to protect your Connected Person's information.

The table of content of this Policy is set out as below:

I. How We Protect Your Connected Person's Information

7. Information security is our top priority. We will always endeavour to safeguard your Connected Person's information against unauthorised or accidental access, processing or damage. We maintain this commitment to information security by implementing appropriate security and managerial measures to secure your Connected Person's information. We will take responsibility in accordance with the law if your Connected Person's information suffers from unauthorised access, public disclosure, erasure or damage for a reason attributable to us and so impairs the lawful rights and interests of Your Company and/or Connected Person.

8. Our website supports advanced encryption technology - an existing industry standard for encryption over the internet to protect your Connected Person's information. When Your Company provides sensitive personal information through our website or applications, it will be automatically converted into codes so as to ensure secure transmission afterwards. Our web servers are protected behind "firewalls" and our systems are monitored to prevent any unauthorised access.

9. We maintain strict security system to prevent unauthorised access to your Connected Person's information. We exercise strict management over our staff members who may have access to your Connected Person's information, including but not limited to access control applied to different positions, contractual obligation of confidentiality agreed with relevant staff members, formulation and implementation of information security related policies and procedures, and information security related training offered to staff.

10. We will not disclose your Connected Person's information to any third party, unless the disclosure is made to comply with laws, regulations and regulatory requirements or according to this Policy or other agreement (if any) or based on Your Company or Connected Person' separate authorisation or consent. When we use services provided by external service providers (entities or individuals), we

also impose strict confidentiality obligations on them and request them to take all data protection measures required pursuant to applicable laws and regulations when processing your Connected Person's information.

11. **For the security of your Connected Person's information, you take on the same responsibility as us. You shall properly take care of your Connected Person's information, including the documents, devices or other media that may record or otherwise relate to such information, and shall ensure such information and relevant documents, devices or other media are used only in a secured environment. You shall not, at any time, disclose to any other person or allow any other person to use such information and relevant documents, devices or other media. Once you think your Connected Person's information and/or relevant documents, devices or other media have been disclosed, lost or stolen, or any other circumstances may otherwise affect your Connected Person's information security have occurred, you shall notify us immediately so that we may take appropriate measures to prevent further loss from occurring.**

12. We will organize regular staff training and drills on emergency response so as to let the relevant staff be familiar with their job duties and emergency procedures. If, unfortunately, a personal information security incident occurs, we will adopt emergency plan and take relevant actions and remediation measures to mitigate the severity and losses in connection therewith. Meanwhile, we will, following the applicable requirements set out in laws and regulations, inform you of the basic information of the security incident and its possible impact, the actions and measures we have taken or will take, suggestions for you to prevent and mitigate the risk, and applicable remediation measures. We will inform you about the security incident by email, mail, call, SMS, push notification or through other methods as appropriate in a timely manner. Where it is difficult to notify each vendor, we will post public notice in a reasonable and effective way. Please inform the relevant affected Connected Persons of the situation in accordance with applicable laws and regulations in a timely manner. Meanwhile, we will report such personal information security incident and our actions to the relevant authorities in accordance with applicable laws, regulations and requirements of the authorities.

II. How We Collect Your Connected Person's Information

5. Personal information refers to any kind of information related to an identified or identifiable natural person as electronically or otherwise recorded, excluding information that has been anonymized. Personal information includes name, birth date, ID certificate information (ID card, passport, etc.), personal biometrics recognition information, contact information, address, account information, property status, location, etc. Sensitive personal information refers to personal or property information that, once leaked or illegally provided or misused, may harm personal or property safety and will easily lead to infringement of the personal

reputation, human dignity, physical or psychological health, or discriminatory treatment. Such information mainly includes ID certificate information (ID card, passport, etc.), personal biometrics recognition information, property information, transaction information, medical and health information, specific identity, financial account, individual location tracking, etc., as well as any personal information of a minor under the age of 14 (i.e. child).

6. **Information We May Need to Collect**

a) When you apply to become our vendor, we may collect the following personal information about Your Company:

Purposes or Functions	Information We May Need to Collect
In order to communicate with Your Company, evaluate and manage vendor setup, conduct due diligence during the vendor on-boarding phase	(1) The name of the Vendor's legal representative. (2) Name, contact information (including fixed telephone number, mobile phone number, email address) and current position of the Vendor's contact person. (3) If the compliance risk rating of the procured services is high or very high after the completion of an internal inherent risk assessment, we need to further collect the name, date of birth, gender, nationality and identity **ID certificate information (including certificate type, number)** of the following individuals: ● the ultimate beneficial owner (natural person) of Your Company who has more than or equal to 10% equity, voting rights or property (including bearer stock, capital and profits) ; ● All senior management and executive directors of Your Company.

b) When Your Company becomes our vendor, we will use the personal information obtained during the above on-boarding process to further manage the conclusion and performance of the relevant agreement between Your Company and us. In addition, we may need to further collect the following related personal information about Your Company:

Purposes or Functions	Information We May Need to Collect
In order to conclude and perform the relevant contracts/	(1) Information about the staff assigned by Your Company to provide on-site services to HSBC • Name, nationality, gender, date of birth, **ID certificate information**

agreements between HSBC and Your Company	**(including certificate type, number, date of expiry, issue country/region),** • As per the service nature, we may further collect background vetting information, including identity verification, working experience, current residential address, **criminal check (where legally permitted or required), any negative news available on public social media, credit reference check (only applicable when your staff have resided in the relevant country/territory for a period of six months or more within the last five years and we are legally permitted to do so),** confirmation of educational and other necessary qualification, **sanction check, any relationship with PEP and relevant information, whether you are subject to any legal or regulatory restriction which may affect your staff's provision of services, entries in local fraud databases (if any).** (2) Other staff and contact person's information provided by Your Company in the process of performing the agreement, including name, contact information (including fixed telephone number, mobile phone number, email address) and current position. (3) If the compliance risk rating of the procured services is high or very high after the completion of an internal inherent risk assessment, we need to further collect the name, date of birth, gender, nationality and **identification certificate information (including certificate type, number)** of the following individuals: • the ultimate beneficial owner (natural person) of Your Company who has more than or equal to 10% equity, voting rights or property (including bearer stock, capital and profits) ; • All senior management and executive directors of Your Company.

7. For the purposes described in this Policy, we may receive and keep the personal information proactively provided by Your Company/Connected Person, or, in accordance with laws, regulations, regulatory provisions, or the authorisation or consent of Your Company/Connected Person, collect, enquire, and verify by proper methods your Connected Person's personal information from/with members of the HSBC Group or other third parties (including but not limited to credit reference agencies, information service providers, relevant authorities, contact persons and other entities/individuals). "HSBC Group" under this Policy means HSBC Holdings plc, and/or any of its affiliates, subsidiaries, associated entities and any of their branches and offices (together or individually), and "member of the HSBC Group" has the same meaning.

8. The personal information we collect may be in paper, electronic or any other forms.

III. How We Use Your Connected Person's information

4. We may use your Connected Person's information for the following purposes:

(1) to realize the purposes and functions mentioned in above Article II of this Policy "How We Collect Your Connected Person's information" and below Article VI of this Policy "Special Circumstances for Information Processing";
(2) to comply with any Applicable Laws ("Applicable Laws" refer to any applicable statute, law, regulation, ordinance, rule, judgment, decree, voluntary code, directive, sanctions regime, court order applicable to any member of the HSBC Group, agreement between any member of the HSBC Group and an authority, or agreement or treaty between authorities and applicable to HSBC or a member of the HSBC Group) and any order or requirement from any authority;
(3) to perform our and/or the HSBC Group's compliance obligations (including regulatory compliance, tax compliance and/or compliance with any Applicable Laws or requirements of any authority), or to implement any policy or procedure made by us and/or the HSBC Group for the performance of compliance obligations.
(4) for our third party risk management, business operations and management needs, including but not limited to monitoring and reviewing HSBC's supplier services procurement process, global operations, system or product development, audit, etc.;
(5) manage financial crime risk, prevent or prohibit illegal or non-compliant activities, control or reduce risks, detect, investigate and prevent any actual, suspected or potential financial criminal activities (including money laundering, terrorist financing, bribery, corruption, tax evasion, fraud, evasion of economic or trade sanctions, and any act or attempt to circumvent or violate any applicable norms relating to such matters) (including the possibility of further inquiries or confirmation of the identity and status of the relevant individuals or entities and whether they are subject to the sanctions regime)
(6) if applicable, collect from you any amounts due and unpaid;

(7) exercise or maintain our rights.

5. **The above information collection and use in this Policy shall not impact our use of your Connected Person's information for purposes as otherwise agreed between you and us.**

6. If we use your Connected Person's information for purposes other than the purposes as set forth in this Policy or in other agreement between you and us, we shall inform you how we use this information and obtain your consent before using your Connected Person's information for such additional purposes as per applicable laws and regulations.

IV. How We Store Your Connected Person's Information

Since we use global purchasing, account payable and risk management system which means that to the extent permitted by regulatory rules and applicable laws, your Connected Person's information may be transferred to and/or stored in the foreign jurisdictions, or be accessed from these jurisdictions. Up to now, the names and contact details of our overseas trustees are as follows: 1) HSBC Global Services (Hong Kong) Limited (contact: hkdpo.enquiry@hsbc.com.hk); 2) HSBC Global Services (UK) Limited (contact: ico.correspondence@hsbc.com). If we transfer your Connected Person's information overseas, we will comply with applicable laws and regulations related to cross border data sharing. Whether it is processed domestically or overseas, in accordance with applicable data protection legislation, your Connected Person's information will be protected by a strict code of secrecy and security which we, other members of the HSBC Group and their staff, and third parties are subject to.

We comply with applicable laws and regulations on data storage and keep your Connected Person's information for the shortest time necessary to meet the purpose of information collection. For example, if we enter a contract with Your Company, any personal information we collect will be retained for 30 years from the expiration date of the contract with Your Company. We have a data retention policy that determines the specific retention period for each type of information based on different service scenarios and the nature of the service. At the end of the corresponding retention period specified in this Policy, we will destroy, delete or anonymize the relevant information. Alternatively, we will store your Connected Person's information in a safe and segregated way when it is impossible to destroy, delete or anonymize your Connected Person's personal information. **The exception is when the information needs to be retained according to applicable laws and regulations, regulatory, archival, accounting, auditing or reporting requirements, special agreement between Your Company and us, or for record checks or enquiries from Your Company, regulators or other authorities.**

V. How We Entrust Processing, Share, Transfer and Publicly Disclose Your Connected Person's information

4. Entrusted Processing and Sharing

For the purposes set out above in this Policy, we may provide or disclose all or part of your Connected Person's information to the following recipients under the preconditions that such provision or disclosure is necessary and is made with proper protective measures (please refer to Article I of this Policy "How We Protect Your Connected Person's information" for details) and the recipients may also, for the aforesaid purposes, use, process or further disclose the information they receive provided that corresponding protective measures are adopted pursuant to the applicable laws or our requirements:

(1) **any member of the HSBC Group;**
(2) **any contractor, subcontractor, agent, third party product or service provider, licensor, professional consultant or associated person of the HSBC Group (including their employees, directors and officers);**
(3) **any regulator of HSBC or any member of the HSBC Group or any other authority, or any organisation or individual designated by such regulators or authorities;**
(4) **anyone acting on your behalf according to your authorisation or in accordance with law (for example your legal advisers, contact persons);**
(5) **any party in connection with the transfer, reorganization, disposal, merger, spin-off or acquisition of business /assets involving us.**

Subject to applicable laws and regulations, we will seek separate consent from Your Company or your Connected Person (if legally required) and notify Your Company or your Connected Person of the data sharing/transferring arrangement, including the data receiver's identity, contact information, the purpose of processing, the method of processing, and the types of personal information.

In case of cross border personal information sharing, we will also conclude a data protection agreement with the offshore personal information recipient and, where necessary, adopt the standard data protection clause formulated by the Cyberspace Administration of China as well as specify your Connected Person's relevant personal information subject's right in his/her capacity as a third party beneficiary under said agreement pursuant to applicable laws and regulations, for example the manner and method of exercising Connected Person's right towards the offshore personal information recipient. If Your Company or Connected Person wants to know more details about aforesaid data protection agreement, please contact us to raise such request via the method listed in Article IX of this Policy "How to Contact Us".

5. Transfer

Without the separate consent of Your Company or Connected Person, we will not transfer your Connected Person's information to any other company, organization or individual, except **in the case of any business/asset transfer,**

restructure, disposal, merger, spin-off or acquisition transactions involving us where the transfer is necessary. In such circumstances, we will inform Your Company or Connected Person of the name and contact method of the data recipient as per applicable laws and regulations as well as request the personal information recipient to continue to protect your Connected Person's information as per applicable laws and regulations. If the personal information recipient changes the data usage purpose and processing method, it shall obtain separate consent from Your Company or Connected Person.

6. Public Disclosure

We will not disclose your Connected Person's information to the public unless we have separate consent from Your Company or Connected Person, except where we are mandatorily required to do so in accordance with applicable laws and regulations, judicial or legal proceedings, or mandatory administrative enforcement by the authorities.

VI. Special Circumstances for Information Processing

We will process your Connected Person's information (collection, storage, use, analysis, transfer, provision, disclosure) based on the consent of Your Company or Connected Person. To the extent allowed by laws and regulations, we may process your Connected Person's information without the consent from Your Company or Connected Person under the following circumstances:

(1) **where it is necessary for entering into a contract or the performance of a contract to which Connected Person is the party;**
(2) **where it is necessary for compliance with a legal obligation to which we are subject;**
(3) **where it is necessary in order to protect Connected Person or others' vital interests related to life and property in an emergency or respond to public health emergencies;**
(4) **where it is within reasonable limits in order to carry out news coverage or media supervision for the public interest;**
(5) **where it is within reasonable range according to law to process the information which has been legally made public or publicized by the Connected Person;**
(6) **other circumstances stipulated by laws and regulations.**

VII. How We Use Cookies and Similar Technologies

3. Your Company or Connected Person visits, browses, uses of any of our website or mobile device applications may be recorded for analysis on the number of visitors to the site and/or applications, general use patterns and specific use patterns of Your Company/Connected Person and improving Your Company/Connected Person's

experience. Some of this information will be gathered through the use of "Cookies" and similar technologies. Such technologies can enable our website or applications to recognise Your Company/Connected Person's device and store information about Your Company/Connected Person's use of website and/or applications so to provide continuous services to Your Company/Connected Person and to tailor the content of our website/applications to suit Your Company/Connected Person's interests. We will be able to access the information stored on the Cookies and similar technologies for aforesaid purposes.

The information collected by Cookies is anonymous aggregated data, and contains no personal information such as name, address, telephone, email and etc.

4. **Most local terminals are initially set to accept Cookies. Your Company or Connected Persons can manage or disable Cookies based on your/their own preference. Should Your Company or Connected Persons wish to disable the Cookies, you or they may do so by changing the setting on your or their local terminals. However, after changing the setting Your Company or Connected Persons may not be able to enjoy the convenience that Cookies bring, but Your Company or Connected Persons' normal use of other functions of your or their local terminals will not be affected.** Different local terminals offer different methods for setting changes, and Your Company or Connected Persons can find information on how to manage cookie settings on certain browsers via the following links.

- Cookie settings in Chrome
- Cookie settings in Firefox
- Cookie settings in Microsoft Edge
- Cookie settings in Safari

VIII. Your Connected Person's Rights Relating to Personal Information

7. Your Connected Persons have the right to request us to protect and secure their personal information in accordance with the provisions of the laws, regulations, and this Policy. They have the right to exercise their rights of individual granted by applicable laws and regulations.

8. Your Connected Persons have the right to check with us whether we hold their personal information as well as to access and copy their personal information.

9. Your Connected Persons have the right to change the scope of authorization or withdraw their consent, and exercise their right per the method listed in Article IX of this Policy "How to Contact Us". We will not further process the related information once Your Connected Persons change their authorization. Please note

the withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.

10. **Your Company has the right and obligation to update your Connected Person's information with us to ensure all information be accurate and up to date.** Your Connected Persons have the right to request us to provide convenience for them to update their personal information with us and to correct any of their personal information that is inaccurate.

11. Your Connected Persons have the right to request us to delete or otherwise properly dispose of their personal information that is beyond the retention period in accordance with the applicable laws and regulations, this Policy, and other agreement between you and us. If we cease our operation, we will stop collecting any personal information of your Connected Person's information in a timely manner, delete or anonymize all your Connected Person's information, and inform Your Company of such operation cessation via courier or public announcement, except as otherwise provided by laws and regulations or where the personal information deletion is technically impossible.

12. Nothing in this Policy shall limit the rights your Connected Person should have as a personal information subject under applicable laws and regulations.

IX. How to Contact Us

1. Requests for access to, copy, correction or deletion of personal information, for change/withdrawal of authorisation or disposal of personal information beyond retention period, or for a copy of this Policy, enquiries about our practices regarding personal information protection or exercising other rights you or your Connected Persons are granted by the laws and regulations, should be addressed to such contact person as listed out in Annex 1.

2. For security purposes, you Connected Persons may need to provide the request in written form via Your Company to prove their identity. We may request Your Company to verify your Connected Persons' identity before processing their request.

3. Upon the receipt of your Connected Persons' request, we will reply to them within 15 working days or shorter period as prescribed by laws and regulations (if any).

4. We will not charge fees for the processing of above-mentioned reasonable requests for checking, correcting or otherwise disposing of your Connected Person's information.

   Notwithstanding the foregoing, we may reject illegal, noncompliant, unnecessarily repeated request, request which needs excessive technical

means (for example, the need to develop information systems or fundamentally change current practices) or brings risks to the legitimate rights and interests of others, or is unreasonable or technically impracticable. Further, we may not be able to respond to part or all of your Connected Person's request under any of the following circumstances:

(1) **Where the request is in relation to our legal and financial compliance obligation under laws and regulations;**
(2) **where the request is in direct relation to state security or national defence security;**
(3) **where the request is in direct relation to public security, public sanitation, or major public interests;**
(4) **where the request is in direct relation to criminal investigations, prosecutions, trials, execution of rulings, etc.;**
(5) **where there is sufficient evidence that Your Company or the Connected Person is intentionally malicious or abuses your/his/her rights;**
(6) **where the purpose is to protect the Connected Person or other individual's life, property and other substantial legal interests but it is difficult to acquire the consent of the Connected Person;**
(7) **where responses to Your Company's or the Connected Person's request will give rise to serious damage to the legal rights and interests of Your Company, the Connected Person or any other individual or organisation; or**
(8) **where the request involves any trade secret.**

5. Your company or Connected Person may supervise or make suggestions for our practices regarding personal information protection, and lodge complaints or demand compensation according to law against us or our staff for any infringement of the rights and interests in your Connected Person's information.

   If your company or Connected Person has any query, complaint, feedback, comment, suggestion, please contact us through the contact information listed in this Policy.

X. Formulation, Effectiveness, Update of this Policy and Others

1. **The Policy is made by us and published on HSBC's relevant vendor management websites and/or applications and takes effect on the date of issuance.** This Policy may be amended and updated from time to time, in particular when the following material changes occur:

   (7) Material changes in our vendor management model or third-party staff information management model, such as changes to the purposes of processing personal information, the types of personal information

processed, the manner in which personal information is used, etc.;

(8) Material changes in our ownership structure, organisational structure, etc., such as changes as result of business adjustments, bankruptcy, mergers, etc.;

(9) Changes in the main recipients to whom personal information is shared, transferred or publicly disclosed;

(10) Material changes in the rights of your Connected Persons relating to personal information or in the methods to exercise such rights;

(11) Changes of our contacts for personal information related requests/enquiries, complaint or feedback channels;

(12) other changes that may have a material impact on the personal information rights and interests of your Connected Persons.

We will post the changes to the Policy or the updated Policy through pop-ups or announcements, etc. on HSBC's relevant vendor management websites and/or applications. Changes to the Policy shall not diminish or limit the rights your Connected Person should have as a personal information subject under applicable laws and regulations.

2. If Your Company or Connected Person is also a customer of the HSBC Group, attention is drawn to the relevant personal information protection policy to customers.

3. Some links in our website may refer to websites of other companies, which may have their own privacy notices. The content may be different with ours. You need to make sure you are satisfied to their privacy notices when you are using other websites.

4. In case of discrepancy between the Chinese and English versions of this Policy, the Chinese version shall apply and prevail.

Annex 1

List of HSBC Group Entities in the Mainland China and Contact Information

	Entity Name	Mailing Address	Zip Code	Contact Person	E-mail	Telephone
22.	HSBC Bank (China) Company Limited	HSBC Building, Shanghai IFC, 8 Century Avenue, Pudong, Shanghai, China	200120	Procurement Department	chn.sourcing@hsbc.com	021-38886325
23.	Beijing Miyun HSBC Rural Bank Company Limited	No.126-1, Xin Dong Road, Miyun, Beijing, China	101500	Procurement Department	chn.sourcing@hsbc.com	021-38886325
24.	Chongqing Dazu HSBC Rural Bank Company Limited	No.1 Beihuan Road(E) , Dazu, Chongqing, China	402360	Procurement Department	chn.sourcing@hsbc.com	021-38886325

25.	Chongqing Fengdu HSBC Rural Bank Company Limited	No.107, Pingdu Avenue(E), Sanhe Town, Fengdu, Chongqing, China	408200	Procurement Department	chn.sourcing@hsbc.com	021-38886325
26.	Chongqing Rongchang HSBC Rural Bank Company Limited	No. 3/5/7, Haitang Er Zhi Road, Changzhou Street, Rongchang, Chongqing, China	402460	Procurement Department	chn.sourcing@hsbc.com	021-38886325
27.	Dalian Pulandian HSBC Rural Bank Company Limited	1-2/F, No. 3 Nanshan Road, Pulandian, Dalian, Liaoning, China	116200	Procurement Department	chn.sourcing@hsbc.com	021-38886325
28.	Fujian Yong'an HSBC Rural Bank Company Limited	No.1211, Yan Jiang Road, Yong'an, Fu Jian, China	366000	Procurement Department	chn.sourcing@hsbc.com	021-38886325

29.	Guangdong Enping HSBC Rural Bank Company Limited	No.44, Xin Ping Middle Road, Enping, Guangdong, China	529400	Procurement Department	chn.sourcing@hsbc.com	021-38886325
30.	Hubei Macheng HSBC Rural Bank Company Limited	No.56 Yurong Street, Macheng, Hubei, China	438300	Procurement Department	chn.sourcing@hsbc.com	021-38886325
31.	Hubei Suizhou Cengdu HSBC Rural Bank Company Limited	No. 205, Lieshan Avenue, Ceng Du, Suizhou, Hubei China	441300	Procurement Department	chn.sourcing@hsbc.com	021-38886325
32.	Hubei Tianmen HSBC Rural Bank Company Limited	Building 3, Yin Zuo Di Jing Wan, Tianmen New City, Tianmen, Hubei, China	431700	Procurement Department	chn.sourcing@hsbc.com	021-38886325

33.	Hunan Pingjiang HSBC Rural Bank Company Limited	Room 101-102 , 106 , Commercial Pedestrian, Pingjiang, Yue Yang, Hunan, China	414500	Procurement Department	chn.sourcing@hsbc.com	021-38886325
34.	Shandong Rongcheng HSBC Rural Bank Company Limited	Room 2, No. 198, Chengshan Avenue (E), Rongcheng, Shandong, China	264300	Procurement Department	chn.sourcing@hsbc.com	021-38886325
35.	HSBC Electronic Data Processing (Guangdong) Limited	4-17/F, Office Tower 2 TaiKoo Hui, No. 381 Tianhe Road, Tianhe District, Guangzhou, Guangdong, China	510620	Procurement Department	chn.sourcing@hsbc.com	021-38886325

36.	HSBC Software Development (Guangdong) Limited	22/F, Office Tower 2, Taikoo Hui, No. 381 Tianhe Road, Tianhe District, Guangzhou, Guangdong, China	510620	Procurement Department	chn.sourcing@hsbc.com	021-38886325
37.	HSBC Life Insurance Company Limited	29th Floor, HSBC Building, No. 8 Century Avenue, China (Shanghai) Pilot Free Trade Zone Shanghai, China	200120	Procurement Department	chn.sourcing@hsbc.com	021-38886325
38.	HSBC FinTech Services (Shanghai) Company Limited	Room 406, No. 859-863, Huanhu West 1st Road, Lingang New	200120	Procurement Department	chn.sourcing@hsbc.com	021-38886325

		Area, Pilot Free Trade Zone, Shanghai, China				
39.	HSBC Insurance Brokerage Company Limited	Room 201, 2F, Tower 3, No.12 Anxiang Street, Shunyi, Beijing, China	101300	Procurement Department	chn.sourcing@hsbc.com	021-38886325
40.	HSBC Corporate Services (Shanghai) Limited	35/F HSBC Building, Shanghai IFC, 8 Century Avenue, Pudong, Shanghai, China	200120	Procurement Department	chn.sourcing@hsbc.com	021-38886325
41.	HSBC Qianhai Securities Limited	Unit 2201, 22/F, Qianhai Chow Tai Fook Finance	518052	Procurement Department	chn.sourcing@hsbc.com	021-38886325

		Tower (Phase I), No. 66 Shu Niu Avenue, Nanshan Subdistrict, Qianhai Shenzhen-Hong Kong Cooperation Zone, Shenzhen, China				
42.	HSBC Philanthropy Foundation Beijing	18/F Fortune Financial Center, No 5 Dongsanhuan Zhong Road, Chaoyang District, Beijing China	Procurement Department	chn.sourcing@hsbc.com	021-38886325	Procurement Department