

花旗对供应商的要求

负责人：
花旗采购与风险主管

发布日期：
2015 年 1 月

修订日期：
2026 年 9 月

版本：
9

目录

1	总体概览	4
2	平等就业机会	5
3	反贿赂和反腐败 (AB&C)	6
4	礼品和款待	6
5	供应商合作与供应商原则	7
6	禁止现代奴役	7
7	供应商人员	9
8	欺诈管理	9
9	媒体互动和公开露面	11
10	书面电子通信	11
11	政治活动和捐款	12
12	反洗钱 (“AML”)	12
13	记录管理	14
14	企业弹性/业务连续性	14
15	全球背景筛查标准	19
16	费用	21
17	信息安全 (IS)	22
18	安全工作场所准则	49
19	人工智能/机器学习 (包括生成式 AI/代理式 AI)	50
20	客户投诉	51
21	个人交易和投资政策	52
22	计费和发票开具标准	52



23	强制休假政策.....	53
	附录 - 定义.....	54

1 总体概览

1.1. 一般要求

本《花旗对供应商的要求》（“要求”）详细列明供应商在与花旗开展业务过程中必须履行的部分义务。某些要求适用于所有供应商，而其他要求对特定供应商的适用性则取决于供应商向花旗提供的产品和服务类型（此类要求在下述第 1.2 节中概述，并在其中列出的每项条款开头注明适用性）。本文中首字母大写的术语，其含义以本文（包括所附附录）中的定义为准；若本文中未作定义，则以相关合同（定义见下文）中的定义为准。

本要求是供应商与花旗签订的协议（包括但不限于交易文件，如工单、许可附表，统称为“合同”）项下的合同义务，是对任何协议中规定的义务、适用法律（定义见下文）项下的义务、花旗告知供应商其义务的任何通知（统称为“通知”），或花旗业务部门或职能部门实施的任何额外、更具体要求的补充。若上述各项要求与本要求之间存在任何冲突，则以限制性更强的义务和要求为准。供应商应采取主动态度，若对本要求（包括其任何变更、任何请求的豁免，或其中任何内容或与适用法律之间的任何潜在冲突）有任何疑问，应咨询其主要花旗业务联系人（或其指定人员）。

供应商应及时配合花旗可能提出的任何合理数据请求，提供花旗为履行适用法律义务所需、且与供应商服务或人员相关的数据。供应商未能履行上述义务，将被视为对本协议条款的实质性违约。

如未能遵守本要求或供应商所对接的花旗业务部门规定的任何附加要求，花旗有权终止与供应商的合同。此外，违反本要求的行为亦可能构成对适用法律的违反，并可能导致供应商对花旗（或第三方）承担民事赔偿责任，或面临刑事处罚。未经花旗银行书面同意，供应商不得以执行自身内部政策为由，替代其遵守本要求各项条款的义务。

1.2. 适用于特定供应商的要求

下表列出了适用于符合该表所述适用性标准的特定供应商的若干要求。下表未提及的各节内容适用于所有供应商。

章节号	章节标题	适用性
2	平等就业机会/平权行动	适用于为履行花旗与美国联邦政府合同所必需的和采购订单；如无法确定相关合同或采购订单是否构成美国联邦政府的分包合同或采购订单，可酌情在条款开头或末尾添加“如适用”字样。
12	反洗钱	适用于履行特定客户相关服务（例如，客户准入、客户账户及交易筛查）或交付与上述活动有关的数据/指标的供应商；和/或作为现金或金融工具（例如，远程存款、快递、运钞车或保险箱服务）中介的供应商。
13	记录管理	适用于访问/处理/存储花旗信息的供应商。
14	业务连续性	适用于提供花旗所使用的服务或托管技术基础设施/应用程序的供应商。花旗业务活动负责人（BAO）负责向供应商传达适用性和 COB 要求。

章节号	章节标题	适用性
15	全球背景筛查标准	适用于向花旗提供服务的供应商。
16	费用	适用于按合同规定有资格要求报销业务费用的供应商。
17	信息安全（IS）	适用于访问/处理/管理/存储花旗信息的供应商（包括分包商）；和/或负责托管面向互联网的花旗品牌应用程序的供应商；和/或连接到花旗网络资源的供应商；和/或需要在无人陪同的情况下进入花旗设施的供应商。
18	安全工作场所准则	
19	人工智能/机器学习（包括生成式 AI/代理式 AI）	适用于在其提供的产品/服务的任何部分中采用花旗所定义的人工智能/机器学习（AI/ML）的供应商。
20	个人交易和投资政策	适用于作为其在花旗工作职责的一部分需要定期访问 MNPI 的供应商。
23	强制休假政策	本政策适用于担任敏感岗位（定义见术语表）的非雇员（“工作人员”）（“敏感岗位工作人员”），以及敏感岗位员工的直属经理和主管（“管理人员”），以及敏感岗位非雇员对应的花旗业务联系人。

2 平等就业机会

2.1 平等就业机会

花旗制定了相关政策，旨在确保所有符合条件的人员，不分人种、肤色、宗教、性别、性取向、性别认同、祖国、公民资格、移民身份、年龄、婚姻状况、遗传信息、残障、受保护退伍军人身份或受法律保护的任何其他特征，都能获得平等就业机会。

供应商应遵守并督促其人员遵守所有适用的非歧视法律和法规的要求，包括但不限于花旗以书面形式通知供应商必须遵守的任何此类法律或法规。

供应商应按照花旗的《美国平等就业机会政策声明》（请参见 www.citigroup.com/global/eeo-aa-policy）进行审查并采取适当行动。

2.2 政府合同

凡为履行花旗与联邦政府的合同所必需的合同及采购订单，均须逐字纳入以下条款，并保留下文所示的加粗格式。（如果不确定其是否为联邦政府分包合同/采购订单，请酌情在条款的开头包括并添加“如适用”。）

【如适用，】供应商将遵守所有适用的联邦反歧视法，并证明其运营的任何项目均不违反任何适用的联邦反歧视法

2.3 政府合同附录

履行花旗与联邦政府的合同所需的合同和采购订单必须在分包合同或采购订单的附录中包含以下通知。（如果不确定其是否为联邦政府分包合同/采购订单，请酌情在下方声明的开头包括并添加“如适用”。）

作为联邦政府承包商，Citigroup 特此代表受保护退伍军人和残障人士向下面签名的承包商或供应商提供我们的平等就业机会义务书面通知。Citigroup 完全遵守《康复法》第 503 条和《越战老兵调整援助法》及其分别位于 C.F.R. 第 41 篇第 60-741 条和第 60-300 条下的适用条例。我们的《平等就业机会政策声明》请参见 www.citigroup.com/global/eeo-aa-policy。有关我们的《平等就业机会政策声明》的任何问题都可以提交给我们政策声明中列出的联系人。

[如适用]，我们要求您根据我们的政策声明和条例采取适当行动。

3 反贿赂和反腐败（AB&C）

花旗为遵守相关 AB&C 法律而制定了相关政策、程序和内部控制措施，并严格禁止任何形式的贿赂或便利费。供应商（包括业务介绍人）、其人员或直接或间接代表花旗行事的任何人，应按照最高的道德标准，以及根据《美国反海外腐败法》（FCPA）、《英国反贿赂法》（UKBA）及其各自修正案以及花旗开展业务所在国家/地区的所有其他适用的当地 AB&C 法律开展活动。

代表花旗开展业务的供应商或其任何人员，或与供应商与花旗的任何协议或关系相关的任何人员不得：（i）向任何人支付、给予、授权或提议任何款项、好处、利益或任何其他有价值物；或（ii）从任何人处收受或接受任何款项、好处、利益或任何其他有价值物，否则上述每一种情况均属违反 FCPA、UKBA 或任何其他 AB&C 法律的行为。供应商及其人员在代表花旗开展活动和交易时，或在开展与供应商与花旗的任何协议或关系有关的活动和交易时，必须遵守相关要求（包括本条款）。供应商及其人员还必须维护 AB&C 合规计划，以及为确保其遵守所有 AB&C 法律而设计并实施的政策和程序。

如需了解花旗 AB&C 计划的概要，请浏览 [Citigroup's Investor Relations](#)（在“花旗政策”下，选择“AB&C 计划”）。

4 礼品和款待

供应商或其人员不得向花旗员工提供礼品或任何有价值物（包括款待），因为这样做会造成实际或表象利益冲突、交换条件，损害员工的诚信或判断，或者以其他不正当方式影响员工的决策或导致员工的行为违背其职责或出现其他违反适用法律的行为。在不限制前述规定的前提下，员工必须遵守 **Gifts and Entertainment Standard** 中“禁止的礼品与款待”部分的规定。供应商及其人员向任何花旗员工提供的非现金商务礼品每日历年每人总计不得超过 300 美元。

当供应商向花旗员工提供商务款待（例如邀请参加餐饮、体育赛事、文化活动或其他类似活动）时，供应商须亲自出席，且该款待须适当、符合惯例、合理，不得奢华或过于频繁。此外，若供应商未出席，则该款待将被视为商务礼品，须按花旗 **Citi Gifts and Entertainment Standard** 规定的申报门槛进行申报。如向任何人提供有价值的物品或诱使他人实施同样行为会构成或可被合理认为构成腐败、不当行为或违反适用法律，供应商不得代表花旗或声称代表花旗，直接或间接向任何人提供任何有价值的物品（包括由供应商自行承担费用或由花旗员工承担费用提供），亦不得诱使他人实施同样行为。

5 供应商合作与供应商原则

花旗通过多项计划与供应商开展合作，提高我们所服务社区的潜在供应商对花旗采购计划的认知。此外，此类合作还旨在发掘具有发展潜力的供应商，尤其是能够提供创新解决方案、应对新兴业务挑战的供应商。有关花旗对供应商期望的更多信息，请参阅 [Doing Business with Citi](#) 网站以下部分中的内容：

[Citi Statement of Supplier Principles](#)
[Citi Sustainable Progress Strategy](#)

6 禁止现代奴役

针对现代奴役和人口贩运可能在其组织内部或其供应链中发生的风险，花旗致力于维护旨在识别和防止这一风险的管理措施。花旗的供应商应遵守下述要求，并制定有效的企业范围的政策、程序和/或惯例，以识别和防止其自身运营和供应链中的现代奴役和人口贩运风险。供应商必须按照花旗的要求填写花旗的企业社会责任问卷（包括提供所需的任何其他信息），以便花旗评估风险敞口和任何潜在的缓解措施，特别是对于高风险行业和地域的供应商。供应商的分包商应遵守相同的流程。

6.1 避免使用童工

供应商不得雇用童工。“儿童”一词是指未达到适用法律规定最低就业年龄的任何人员；如适用法律未规定最低就业年龄，则指未满 15 周岁或未达到完成义务教育年龄的人员，以两者中年龄较大者为准。在严格禁止使用童工的前提下，如雇用未满 18 周岁的员工，应特别关注其所从事的工作职责及工作条件，确保其不会因工作或工作条件而直接或间接遭受身体、精神或其他方面的伤害。

6.2 自由选择就业

供应商应确保员工不会遭受强迫劳动、精神或身体胁迫、债务劳役、契约劳役、非自愿监狱劳动或奴役贩运，也不会以任何形式被迫劳动，包括强制加班。所有工作均须基于自愿。供应商在本条款下的义务包括但不限于确保以下各项：

1. **合同、工资和工时：**员工应获得以书面形式清晰载明的雇佣或聘用条款，该文件应易于员工理解，并明确列明其权利和义务。该书面文件应包括但不限于关于工资、加班费、付薪周期、工时以及休息时间和节假日权利的透明条款。此

类书面条款应在员工开始工作前提供，雇主应予以遵守，且须符合工作所在地的行业标准及适用法律和集体协议规定的最低要求。

2. **自由终止工作的权利：**员工有权根据适用法律和集体协议，在按照适用法律和集体协议规定的合理通知期后，自由终止其雇佣关系，且不得受到任何不当处罚。
3. **不人道待遇：**员工、其家属及与其密切相关的人员不得遭受苛待或不人道待遇，包括但不限于体罚、身体、心理或性暴力或胁迫、言语辱骂、骚扰或恐吓。移民员工、其家属及与其密切相关的人员不得因其国籍而在工作条款或工作条件方面受到歧视。
4. **工资、福利和工时：**薪酬应符合所有适用工资法律的规定，包括与最低工资、加班时间和法定福利相关的法律。员工应获得足额、按时支付的工资，并附有透明的工资单。不得将扣减或扣押工资或福利作为纪律处分措施。每周工作时长不得超过当地法律规定的上限，加班必须出于自愿，且在法律允许的范围内，拒绝加班不得受到惩罚。
5. **不得没收身份证件：**不得以雇佣条件为由没收或扣留员工的身份证明、旅行证件、护照或其他官方文件或任何其他贵重物品，也不得直接或间接利用扣留财产限制员工的自由或制造工作场所奴役。
6. **不得收取招聘费用或导致债务束缚：**与招聘员工相关的任何费用或成本（包括但不限于工作签证费、差旅费和文件处理费）均不得直接或间接向员工收取。同样，不得要求员工支付具有在工作场构成奴役行为的意图或效果的款项（包括保证金），或要求员工通过工作偿还债务。如果经查实，供应商向员工收取了与招聘流程相关的费用或成本，或者在雇佣期间产生了此类费用或成本，供应商应采取合理措施，确保相关费用得到及时退还或补偿。如需通过第三方（如职业介绍所）招聘员工，则只应选用信誉良好的职业介绍机构。如需直接招聘员工，则只应选用信誉良好的招聘机构。禁止向员工收取招聘费用的规定适用于所有招聘机构、代理机构和分代理机构。供应商应建立相应的控制措施，以确保合规。
7. **行动自由：**员工应享有自由行动的权利，不得受到不合理限制，也不得被以任何形式限制在工作场所或其他由雇主控制的场所（例如宿舍楼）。除非因执行工作的地点或性质确有必要，否则不得要求员工必须居住在雇主控制的场所。
8. **申诉不受报复：**员工可就雇主所给待遇向雇主表示不满，且不会因为提出不满而遭受损害、报复或伤害。

7 供应商人员

7.1 供应商的人员培训、分配、重新分配和管理

供应商将聘用足够数量的经过适当培训和教育、拥有经验和技能的人员，以符合任何合同的最有效方式履行服务，并将按要求证实此类人员的资格。在将人员分配到项目之后，未经花旗事先书面同意，供应商不得重新分配或利用任何人员从事其他会减少其项目参与程度的事项，并且在分配项目人员时，通常要尽量减少由于需要重新培训而导致的中断。供应商将确保其人员不会将自己视为花旗的员工或代理，也不会出于任何目的设法享受花旗员工的待遇，包括要求享有花旗提供的附加福利或失能收入、社会保障税或福利、联邦失业税、州失业保险福利或联邦所得税预提扣缴。供应商单独承担与其人员有关的所有涉及雇主的责任，包括但不限于以符合供应商作为独立承包商身份的方式保持所有必要的保险范围、提交所有适用的纳税申报表并支付所有必要的税款和保证金。

7.2 更换供应商人员

如果花旗因任何非歧视性原因通知供应商某位人员不为花旗所接受，则供应商应移除和更换已指派给项目的该人员。此外，供应商还同意：如果某位人员无法或不愿意及时、专业地提供服务，则供应商会立即移除和更换已指派给项目的该人员，并禁止其向花旗提供服务（或负责服务的交付或监督）。

7.3 供应商的人事政策

供应商表示、保证和承诺，维护并有效管理全面政策和程序，确保作为自然人并被指派为花旗提供现场服务的人员符合资格，而且此类政策和程序包括工作许可验证、工作经历和刑事定罪背景核查（如下文所述）以及录用前药物检测，前提是这些均在适用法律和任何适用劳资协议允许的范围内。在不限制上述规定普遍性的情况下，供应商进一步声明、保证和承诺，其已建立相应的控制措施和程序，以确保自身完全遵守所有与移民相关的适用法律，包括核实所有指派给花旗的供应商人员均已获得授权，可在整个工作安排期间完全遵守所有与移民相关的适用法律。如有要求，供应商将立即向花旗提供所有分配给花旗的供应商人员的工作授权书面证明，以及供应商遵守与移民相关适用法律的证明。对于任何不具备符合适用法律要求的工作授权的人员，供应商应予以替换，并提供具备适当资质的替代人员，包括提供所有必要的培训和指导，以确保及时有效地提供服务，且上述所有措施均无需花旗承担额外费用。

7.4 供应商所有权

为了遵守花旗开展业务所在司法管辖区的适用法律和法规，供应商有义务应花旗的要求提供自然人和/或实体身份所有者的详细信息，包括供应商的直接所有者，直至并包括通过影响或其他手段直接或间接拥有或控制业务、产品或服务的最终受益所有人。

8 欺诈管理

本条与花旗为识别和降低欺诈风险而采取的措施（“欺诈管理”）相关。

8.1 所有供应商应：

1. 在法律允许的最大范围内，配合花旗对疑似或被指控盗窃、欺诈或其他潜在犯罪活动或不当行为开展任何调查，以及配合花旗对欺诈或犯罪行为的任何起诉。
2. 确保通过 [Ethics Hotline](#) 及时向花旗举报和转介任何潜在的欺诈事件。其中包括但不限于涉及花旗、花旗员工、花旗供应商或代理或非花旗员工（例如临时工和承包商）尝试、疑似、被指控或实际的偷窃、欺诈（例如故意提交有关供应商、计费方案、资金/证券消失等方面的虚假、不准确或失实数据）、犯罪活动或不道德行为。
3. 允许花旗及其代表进行监控和监督，并支持花旗和执法部门对涉及供应商的潜在欺诈活动进行调查。
4. 及时报告供应商获悉的任何利益冲突（包括供应商/供应商员工和/或花旗员工之间的利益冲突）；以及
5. 在花旗的供应商支付系统中设置或更新供应商银行账户的过程中，支持花旗的欺诈预防流程。

8.2 除此之外，如果供应商所提供的服务本身更容易面临欺诈风险，则供应商需要：

1. 记录并遵循欺诈风险管理计划，该计划可识别与向花旗所提供服务相关的重大欺诈风险以及规避这些风险的既有控制措施和程序。
2. 完成欺诈防范培训（在聘用之后 90 个日历日内进行，之后每年一次），并针对向花旗提供的特定服务相关欺诈风险的特定要素对员工进行培训。
3. 监控欺诈未遂实例并保持有效的控制措施，以规避向花旗所提供服务的欺诈风险，记录控制措施的程序并持续测试控制措施的有效性，同时向业务活动负责人（BAO）报告任何缺陷。
4. 针对业务活动负责人（BAO）面临的欺诈风险敞口，提供开展尽职调查/持续监控/评估时所需的任何必要信息。
5. 尽职调查包括第三方欺诈影响评估模板（“TP-FIAT”），该模板旨在对供应商与欺诈风险缓解相关的能力进行控制评估。此操作程序描述了一组由业务活动负责人（BAO）或第三方管理官（TPO）以及欺诈风险管理官（“FRMO”）执行的步骤，以识别和管理欺诈风险。

8.3 自身具有较高欺诈风险的供应商包括但不限于符合下列特征的供应商：

1. （在不受花旗直接控制或监督时）有权访问归类为“机密”或更高级别的数据，并且该访问权限可被用于实施欺诈，例如访问内部账户、金融交易和现金交易；
2. 与花旗网络/系统相连接；以及
3. 提供、支持或访问的服务和功能可能成为实施或实现欺诈的目标，包括：

a) 识别、登记或处理新客户的申请；

- b) 花旗或客户付款/转账活动，和/或对访问这些服务的花旗客户进行身份验证；
- c) 制作、核对或完成对花旗数据或花旗客户（例如，人口统计）数据的更改；
- d) 提供、维护或授权交易工具（例如，借记卡/信用卡、电子钱包、支票簿等）；
- e) 向花旗提供或支持与欺诈事件的预防、检测或应对相关的运营欺诈管理活动；
- f) 提供获得现金、金融票据和资产/实物的实体渠道；
- g) 在无人陪同的情况下或非营业时间进入花旗设施；
- h) 财务报表：会计活动，例如将分录过账到总账/明细账；
- i) 赚取和兑换激励活动奖励。

9 媒体互动和公开露面

花旗企业服务和公共事务部是获得授权，可以代表花旗发布新闻稿或公开声明的唯一部门。供应商发布的任何新闻稿不得直接或间接提及花旗、供应商和花旗之间订立的任何合约或协定，或花旗向供应商采购的任何产品和服务。未经其主要花旗业务联系人的事先书面批准，供应商不得与客户、花旗员工、其他花旗供应商、供应商的其他客户或任何其他第三方开展任何与花旗相关的公共关系活动。

未经各自的主要花旗业务联系人和国家/地区公共事务高级职员的事先书面批准，供应商不得在刊发或发布任何材料（包括书籍、文章、播客、网络直播、博客、网站发帖、照片、视频、社交媒体或其他媒体）、举办或发表演讲、接受采访或公开露面时，以书面或电子格式提述花旗、花旗的业务、客户、产品或服务。

不论是否与向花旗提供服务或产品有关，如未（针对每种情况）获得花旗的事先书面同意，供应商均不得使用花旗专有标记、商标、服务标志、商号、徽标、符号或品牌名称。供应商不得使用花旗的名称、徽标或商品、设施或关系牟利，或在花旗以外的工作中使用（包括用在信笺抬头或个人网站、博客或其他社交网站上）。此外，供应商不得将花旗的名称、设施或关系用于任何慈善或公益目的。

10 书面电子通信

在与花旗人员互动时，或在为花旗或代表花旗履行其义务时，仅允许供应商使用花旗批准的书面电子通信设备、系统和服务。全新、扩展或改进的花旗电子通信渠道，无论作为独立工具还是集成到更广阔的平台，亦无论由花旗提供还是由第三方提供，均必须按照供应商已由其 BAO 予以书面通知的适用花旗要求进行批准。禁止在未经花旗批准的消息传递平台（如 WhatsApp、微信、LINE、Slack、Signal、Telegram、iMessage、SMS、Viber 以及任何其他交互式电子平台）上与花旗人员沟通花旗业务。

此外，对于通过花旗提供的通信设备、系统和服务创建、发现、使用、访问、下载、存储、传输、接收或删除的书面电子通信，供应商不应对其抱有任何隐私期待。花旗可以

监控电子通信设备、系统和服务以及电子通讯。此类电子通讯归花旗所有，并可根据适用的记录保留要求予以保留（须遵守当地法律和法规）。

<https://policydirectory.citi.net/cpd/layouts/15/DocIdRedir.aspx?ID=CPDPROD-13-8739>

11 政治活动和捐款

各种法律，例如与以下方面相关的法律：外国影响、竞选经费、礼品和款待、立法、基层、商誉和监管游说、采购、付费入场及证券，均规范花旗及其供应商的政治活动和与此类活动有关的披露。供应商未遵守相关花旗政策或准则、法律或法规的任何政治活动均被禁止。

政治活动包括但不限于：

1. 代表竞选公职的候选人、政党委员会或政治委员会提供企业或个人政治捐赠，或为政治捐赠筹集资金，使用公司资金或资源（例如设施、设备、软件或人员），或在公司营业时间提供义务服务；
2. 直接或通过第三方间接游说或从事针对公职人员的宣传活动，包括试图影响官员、立法，在某些司法辖区，还包括试图影响政府机构的规则制订或政府合约的授予；或
3. 寻求、接受或任职于任何与政府有关的政治职位，包括任何政府管理委员会、委员会或其他类似组织中的职位。

未经花旗政府事务全球运营控制部门（ggacontrol@citi.com）的事先书面授权，任何供应商不得代表（或声称代表）花旗或其客户从事或进行任何政治活动。尽管花旗可能会为供应商提供的签有合同并允许的政治活动服务（例如游说）支付费用和/或报销自付费用，但花旗概不会为供应商或其任何员工报销任何类型的个人或企业政治捐赠。

12 反洗钱（“AML”）

适用于履行特定客户相关服务（例如，客户准入、客户账户和交易筛查）或交付与上述活动有关的数据/指标；和/或作为金融交易或工具（例如，远程存款收集、快递、装甲车或保险箱服务）中介的供应商。

12.1 反洗钱义务：

1. 遵守花旗流程和适用法律：

- 维护并遵守花旗旨在满足适用法律要求的各项流程和程序，包括：（i）《格雷姆-里奇-比利雷法案》及其相关法规；（ii）《美国爱国者法案》及其相关法规；（iii）任何有关洗钱的法律或法规；以及（iv）任何与经济制裁相关的法律或法规。此类政策和程序将明确反洗钱方面的角色和责

任，包括要求及时报告任何与金融活动、交易和现金收入相关的异常或潜在异常情况。

2. 人员年度培训及项目要素：

- 确保向花旗提供服务的人员接受针对反洗钱角色和责任的年度培训，包括要求及时报告任何异常或潜在异常的金融活动、交易和现金流入。培训内容应包括但不限于以下方面：
 - a. 可疑活动的报告和上报。
 - b. “了解你的客户”（KYC）计划，包括客户身份识别程序（CIP）、制裁名单和姓名筛查、客户尽职调查（CDD）、强化尽职调查（EDD）以及**最终受益所有人（UBO）**的识别和核实。
 - c. 对所有相关金融工具和活动的交易监控。
 - d. 定期报告/指标，包括法律法规变更和反洗钱计划重大变更的相关报告。
 - e. 反洗钱计划有效性的测试和控制，包括实地视察。

3. 遵守合同条款：

- 遵守合同中关于供应商必须实施的任何计划的规定。

4. 及时报告疑似违规行为：

- 及时以书面形式向花旗报告任何疑似违法行为，包括任何与现金流入、金融活动或涉及花旗或其客户的交易相关的异常或潜在异常活动。

5. 防止和举报偷税漏税：

- 遵守开展业务的国家/地区的所有适用税收法规。
- 任何情况下，供应商都不得参与故意非法偷税漏税行为，或代表他人为此行为提供便利，这可能包括参与协助逃避缴纳到期应付税款或向税务部门隐瞒信息的活动。
- 因此，供应商应采取与偷税漏税有关的合理防范程序，并在发现任何与花旗相关的违法或疑似违法行为时立即以书面形式向花旗报告。

12.2 供应商内部政策和程序：

供应商应制定并维持适当的内部政策和程序，以遵守所有现行或今后生效的反洗钱法律和法规。

13 记录管理

适用于访问/处理/存储花旗信息的供应商。

花旗要求保管花旗信息的所有供应商与其业务活动负责人（“**BAO**”）或主要花旗业务联系人合作，以（i）出于花旗的记录管理目的，将信息识别和归类为“记录”或“临时信息”；（ii）按照花旗主记录目录（“**MRC**”）对记录进行归类；（iii）根据保留要求保留信息；（iv）如无“信息保留”要求，则在信息生命周期结束时妥善处置信息。

BAO 或主要花旗业务联系人必须与供应商合作，以确保供应商已根据 **MRC** 中的花旗记录代码对记录进行识别和归类，并至少每年更新一次详细清单。供应商有义务遵守 **BAO** 传达的记录管理要求。符合处置资格标准的记录必须尽快进行适当处置，但最久不得超过满足保留要求后六个月，除非必须进行“信息保留”。临时信息必须在其最后一次使用后两年内销毁，除非必须进行“信息保留”。包含个人信息的临时信息一旦达到收集目的必须删除，除非必须进行“信息保留”。接到“信息保留”通知后，供应商必须暂停销毁或更改花旗信息。如果有任何疑问，供应商须与其主要花旗业务联系人或 **BAO** 进行核实。

按季度对“国家/地区保留计划”中所列的保留规则进行审查并根据需要加以更新，以符合 **DRIM** 的监管和内部变更。如果存在影响供应商的变更，**BAO** 将通知供应商。供应商必须评估影响，并在相应的系统、流程和清单中实施变更。收到 **BAO** 通知之后的 90 天内所拥有和管理的记录类型。

代表花旗维护文件的供应商负责在 **BAO** 要求的时间内保留（“保存”）、收集和生成被认为与法律或其他程序相关的所有信息。供应商应根据适用的合同条款，按要求向花旗提供相关信息。未经其主要花旗业务联系人或 **BAO** 批准（批准中必须包含下列确认信息：针对到期处置的信息并无有效的“信息保留”要求），供应商不得处置任何花旗信息，不论其分类（如机密、非机密）如何。除非就其他条款达成一致，否则记录管理和保留要求及所有其他的信息处理要求应在合同终止或到期后继续有效。

对于负责监督供应商所保管花旗信息管理措施的供应商人员，供应商应保留列明所有此类人员的文件，并与其主要花旗业务联系人或记录管理员定期举行会议，审查和更新联系人姓名、程序细节、角色和责任，以及花旗供应商记录清单。

14 企业弹性/业务连续性

适用于提供花旗所使用的服务或托管技术基础设施/应用程序的供应商。花旗业务活动负责人（**BAO**）负责向供应商传达适用性和 **COB** 要求。

14.1 恢复资源

供应商的业务连续性计划须提供备用资源，以便在供应商的主要地点中断经营时向花旗提供所有产品和服务。恢复资源所在的地理位置必须与主要地点相距足够远，以最大限度地减少或消除同一灾难事件同时影响主要地点和恢复地点的威胁。

1. 恢复资源不只限于信息系统，还包括向花旗继续提供产品和服务所需的所有资源，包括员工、建筑物、业务设备、数据中心、数据和语音网络以及运输服务。
2. 应用程序的供应商可实现热备份（Hot/Hot）类型的架构，以确保高可用性（HA）配置。此架构要求有两个（至少）相同配置的系统启动并运行，可供客户端/用户使用。此模式提供的最重要的特性在于备用环境与主要（生产）数据中心并发运行。

14.2 恢复服务水平

供应商的业务连续性计划必须符合设定的服务级别，才能对花旗生效。供应商的灾难恢复计划至少应确定以下各项的具体值：

1. 恢复时间目标
2. 恢复时间点目标
3. 恢复资源/技术能力
4. 恢复持续时间

14.3 灾难恢复计划

供应商将制定并维持灾难恢复计划，以确保业务连续性（并可在花旗要求的情况下提供其当前和定期测试的证据），以便即使供应商在某一特定地点开展业务或依靠某些特定人员提供产品/服务的能力受到任何干扰，供应商也能够及时从备用地点或通过替代人员提供产品/服务并履行其义务。灾难恢复计划的副本必须在花旗与供应商之间签订每一份工作订单的生效日期后十（10）个日历日内提供给花旗，之后在每一份工作订单生效期间，每年提供一次。在供应商启动其灾难恢复计划的情况下，供应商将向花旗提供任何必要的说明或其他信息，以便花旗继续接受供应商提供的产品/服务。供应商表示、保证并承诺其灾难恢复计划至少包括以下方面：

1. 旨在缓解包括技术不可用（拒绝服务/DoS）、主要工作地点不可用（拒绝进入/DoA）以及员工不可用（包括分包商）在内的中断影响的恢复程序和策略，包括搬迁、工作转移和/或远程访问；
2. 由供应商维护（包括但不限于）与产品/服务地点处于不同位置的备用灾难恢复站点，将备份介质存储在与产品/服务地点处于不同位置的地点，采用冗余通信线路和服务器；
3. 用于产品/服务的运行和应用的备份/恢复程序，包括详细的书面计划，以应对因电源故障、系统故障、自然灾害或其他无法预见的情况所导致的产品/服务长时间中断，其中包括在双方商定的时间段内恢复运营的流程和程序；
4. 所有内容的保护程序；
5. 备用设备（例如计算机设备）的相关程序和任何第三方协议；

6. 任何场外生产设施的相关程序；以及
7. 供应商的灾难恢复计划应包含以下内容：
 - a. 如果任何灾难可能对产品/服务产生负面影响，供应商将及时通知花旗；
 - b. 供应商应在上述通知之后 24 小时内，向花旗提供通过替代处理设施继续提供产品/服务的计划；
 - c. 产品/服务必须在规定的恢复时间目标（RTO）内全面运行。如果未在适用的合同中另外定义，重要等级被花旗定为“企业关键”或“高”的流程，RTO 为 4 小时或更短；重要等级被花旗定为“中”的流程，RTO 为 24 小时或更短；重要等级被花旗定为“低”的流程，RTO 为 72 小时或更短；以及
 - d. 如果供应商的部分设施无法使用，则供应商为花旗提供的待遇，应不亚于供应商为其他商业客户提供的待遇。

14.4 适用于托管服务的灾难恢复计划要求

在供应商管理并向花旗提供托管服务的范围内，以下规定也应适用。灾难恢复计划应至少包括：

1. 用于托管服务运行和应用的备份/恢复程序，包括详细的书面计划，以应对因电源故障、系统故障、自然灾害或其他无法预见的情况所导致的服务长时间中断，其中包括在双方商定的时间段内恢复运营的流程和程序；
2. 此外，供应商的灾难恢复计划应包含以下内容：（a）供应商应在任何可能对托管服务造成负面影响的灾难发生后两（2）小时内以书面形式通知花旗；（b）供应商应在此类通知之后 24 小时内向花旗提供通过替代处理设施继续提供托管服务的计划，以及（c）托管服务必须在初始通知之后 48 小时内全面启动；
3. 供应商同意根据要求发布必要的信息，以确保花旗制定灾难恢复计划和业务连续性计划，此类计划将与供应商的灾难恢复计划和业务连续性计划相互配合；以及
4. 如果供应商的部分设施无法使用，则供应商为花旗提供的待遇，应不亚于供应商为其他商业客户提供的待遇。

14.5 灾难恢复计划的变更

供应商可以变更其灾难恢复计划，但变更不得以任何可能对服务产生不利影响的方式降低灾难恢复计划的有效性（例如，延长恢复时间目标）。供应商应及时向花旗传达其灾难恢复计划中的任何变更，并应花旗要求对变更予以解释，以便花旗充分了解并能够应对变更。

14.6 分包商的灾难恢复计划

供应商将确保供应商的任何分包商制定并维持符合《花旗对供应商的要求》的灾难恢复计划和相关业务连续性控制措施。供应商必须对分包商进行适当监督，包括定期审查此类控制和测试结果，并确保及时整改发现的任何缺陷。

14.7 灾难恢复计划启用和危机通知

供应商应在以下情况下及时通知主要花旗业务联系人：

1. 供应商启用其灾难恢复计划时；以及
2. 供应商或其分包商面临的、很可能对向花旗提供的服务或产品产生不利影响的任何危机、威胁、前兆警报或网络事件。

14.8 测试

供应商的所有恢复资源和计划必须在生产实施后的 120 天内（对于被花旗归类为“企业关键”的应用程序，则为 90 天）进行测试，并至少每年（每 12 个月）测试一次。测试应证明，供应商能达到向花旗提供的所有产品和服务的恢复服务水平。这些测试必须全面，并应覆盖供应商向花旗提供的全部服务范围。如果要测试向花旗提供的产品/服务的恢复情况，供应商须至少提前 30 个日历日通知花旗。花旗可参与或监督供应商对花旗所使用的应用程序的恢复测试，以验证应用程序在恢复环境中的业务功能。如果花旗希望参与，则供应商应在进行测试之前向花旗提供测试目标、测试计划和连接到测试站点的程序。在完成每一项测试后的十（10）个工作日内，供应商应向花旗提供测试目标、测试计划和测试结果的摘要，包括恢复所需的时限和测试结果的证据（例如屏幕截图）。

14.9 容量验证

对花旗归类为“企业关键”的应用程序进行托管的供应商必须证明可在其 COB/灾难恢复环境中处理生产容量。花旗和供应商必须就验证所采用的方法达成一致。

14.10 使用花旗系统提供服务

如果花旗或花旗关联公司提出要求，则使用花旗系统的供应商将参与（免费或由花旗承担费用）花旗的灾难恢复演练。

14.11 处理测试结果

如果供应商测试的结果表明未达到任何测试目标或任何适用的 RTO，供应商将执行原因分析并及时纠正所发现的任何缺陷。在实施此类纠正后，供应商应在最初测试失败后（或相关工作订单中指定的时限）的一百二十（120）个日历日（对于被花旗归类为“企业关键”的应用程序，则为 90 个日历日）内进行重新测试。

14.12 危机管理

供应商应在其业务连续性计划之外，制定危机管理计划，以指挥和控制恢复操作。供应商的危机管理计划至少应包括以下内容：明确指定具备充分授权、负责启动恢复工作的具体人员；定义用于收集、汇总及分发危机信息的沟通与升级机制；以及建立在发生危机事件时与花旗进行沟通所需的通知和升级流程。

14.13 业务连续性评估

供应商须遵守花旗的第三方业务连续性评估流程，此流程会针对与业务连续性相关的花旗要求以及（适用于花旗或供应商的）任何法律和/或监管要求的遵守情况对供应商政策、程序和控制措施进行评估。评估包括要求供应商回答并提供支持证据的问卷调查，并可能包括对供应商的实地考察。如果评估的调查结果披露或表明存在问题或疑虑，花旗会记录调查结果，并与供应商合作确定纠正问题的方法。供应商必须尽快做出必要的纠正和/或增加补偿控制措施来解决花旗的疑虑，达到合理的满意程度。

14.14 运营弹性

关键业务服务是指如果中断交付可能会对花旗、其客户或金融系统造成重大负面影响的业务。供应商应确保，任何由花旗不定期指定、构成关键业务服务或支持花旗提供关键业务服务的服务要素（“关键业务服务”）的交付中断，不得超过花旗设定的时限，或以其他方式违反花旗不定期通知供应商的任何相关指标（“影响容限”）。影响容限将以明确、有时限的指标表示，该指标代表服务交付可能中断的时间长度。作为持续性合同管治流程的一部分，花旗和供应商应每年对影响容限进行审查。如果由于多个监管机构的要求，花旗需要为单项关键业务服务设定多个“影响容限”，则花旗可为此类关键业务服务单独指定影响容限。供应商应做到以下方面：

1. 如果意识到未能（或很可能无法做到）在花旗设定的相应影响容限范围内交付任何服务，则供应商应立即通知花旗，并附有任何预期或实际失败的原因说明以及为减轻此类失败的影响而采取的措施；
2. 如果收到要求，则供应商应向花旗提供合理协助，以便花旗能够确认所需的人员、流程、技术、设施和信息，进而供应商可交付支持关键业务服务的业务；
3. 向花旗提供合理协助，以便花旗能够开展以下工作：
 - a. 在花旗自身或供应商的运营发生严重但貌似合理的中断的情况下，对供应商保持在每一项关键业务服务的影响容限范围内的能力进行任何内部情境测试；以及
 - b. 在情境测试之后吸取任何经验教训，以便花旗能够确认不足之处，以及为提高供应商有效应对未来中断并从中恢复的能力所要采取的任何必要措施。

如果花旗通过任何内部情境测试，确认供应商在花旗设定的相应影响容限范围内交付服务的能力存在漏洞或局限性，以及供应商未能在花旗设定的相应影响容限范围内交付任何服务，双方将商定一项计划（包括实施该计划的时间表），以确保供应商采取必要措施解决或减少此类漏洞或限制，或弥补失败的原因，从而在合理可行的情况下尽快保持在影响容限范围内（如适用）。

14.15 托管安排

应花旗的要求，以下供应商：（i）向花旗提供软件授权以便其在花旗环境中运行的供应商，或（ii）向花旗提供托管服务的供应商，应确保将存放材料存入花旗指定的托管代理机构，并根据适用的托管协议，就该存放材料签署托管代理机构要求的存放人登记表或其他表格。此后，在有关授权或托管服务的适用协议的剩余期限内，供应商将在托管代

理机构存放寄存材料的更新版本，以确保托管源代码和其他寄存材料与适用于花旗当前使用的软件或托管服务版本的最新版本的软件保持同步。源代码或其他寄存材料更新应在对已授权花旗使用的软件进行任何更新或对花旗所使用的托管服务进行修改之日起三十（30）天内提交给托管代理机构。供应商将全面遵守托管协议中规定的寄存者的所有义务和要求。供应商单独承担所有托管成本和费用，包括但不限于配置费、年费、寄存费、服务费以及任何其他托管费用和成本。在出现发布事件的情况下，托管代理机构应根据基础协议和托管协议的条款向花旗或花旗的指定人员发布寄存材料。

如果源代码（或其他寄存材料）由供应商或托管代理机构根据适用的托管协议履行其义务时直接交付给花旗或花旗的指定人员，则源代码和寄存材料受供应商和花旗之间相关协议下现有授权的约束；前提是每项授权被视为允许花旗在合理必要时使用和修改源代码和其他寄存材料，以便：（i）将软件和其他寄存材料与花旗的系统进行集成并确保兼容性；（ii）确保软件或其他寄存材料符合适用法律、行业标准或市场惯例；（iii）确保软件或其他寄存材料与技术创新保持同步；（iv）确保软件和其他寄存材料能够在现有授权范围内实现花旗及其附属机构的业务目的。任何包含由花旗或代表花旗使用源代码所进行修改的软件版本均受本节所有条款和基础协议的约束；但前提是供应商对任何修改没有权利、所有权或利益，并且与任何修改有关的所有知识产权只归属于花旗。

供应商将采取商业上合理的努力，与提供软件系统中所使用的任何软件的第三方进行协调，以允许供应商在源代码寄存中存放此类第三方软件的源代码。如果第三方拒绝授予供应商此项权利，则供应商应通过商业上合理的努力，在发布事件之后将适用的第三方软件许可协议转让给花旗。

按照本节的要求交付给花旗的源代码应遵守适用的已授权软件或托管服务的现有授权，前提是花旗可根据其业务和运营要求使用和修改源代码及软件系统，以确保软件系统与技术创新保持同步并符合适用法律。任何包含由花旗或代表花旗使用源代码所进行修改的软件版本均受适用协议所有条款的约束；但前提是供应商对任何修改没有权利、所有权或利益，并且与任何修改有关的所有知识产权只归属于花旗。

15 全球背景筛查标准

适用于所有向花旗提供服务的第三方供应商。

15.1 概述 - 背景筛查

背景筛查必须符合所有适用的当地法律法规。本文件中所述的所有信息和自我披露必须由供应商代表、供应商人员以及分包商（视情况而定）提供。无论何时发现，在简历、面试、入职表格或入职流程中提供虚假或遗漏信息，均可能构成花旗根据当地法律拒绝或终止录用的理由。若执行的任何筛查发现不良结果，则不论何时发现，根据当地法律亦构成花旗拒绝或终止任命的理由。

有关背景筛查完成情况的更多信息，请参阅

https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf。

15.2 基本信息的收集和身份验证

在任何供应商人员开始执行花旗任务之前，供应商须收集该人员的姓名、邮寄地址和永久地址（如两者不同）、电话号码和电子邮件地址（如适用）。供应商人员还须提供可验证其身份的文件。这可能包括提供国民识别号码的相关信息和/或文件、政府颁发的带照片身份证或护照。

15.3 制裁筛查

所有代表花旗工作的供应商人员，或持有花旗供应商 25%或以上所有权的负责人（包括分包商），无论其是否有权访问花旗的数据/系统/网络和/或进入花旗办公场所，均须根据美国财政部海外资产控制办公室（“OFAC”）的特别指定国民和被冻结人员（“SDN”）名单以及受美国制裁的地区和司法管辖区名单（“美国制裁”）接受筛查，同时还必须根据美国境外当局发布的任何名单和受制裁的司法管辖区名称接受筛查，包括欧盟（“EU”）综合金融制裁名单、联合国（“UN”）安全理事会综合名单、英国（“UK”）制裁名单以及根据适用于当地司法管辖区的法律法规制定的名单（“非美国制裁”）。

OFAC 名单可在以下网站公开查阅：<https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>。

15.4 移民合规

供应商必须证明其已建立并实施相关规程，以核实所有人员均已获得在任务所在国工作的授权。此外，供应商还必须：（1）确保所有人员均已获得工作许可；（2）遵守所有适用的法律、法规和政策（包括就业资格和核实要求）。供应商还必须建立并维持相关规程，以确保其人员在其他方面遵守所有适用的移民法律和法规，并确保其人员持有与其所从事的任务和活动相适应的签证身份/类别。

15.5 工作经历

如果当地法规有要求，供应商须核实其人员在过去七（7）年或 10 年内的工作经历。必须核实人员的工作经历，确保雇主、职位、日期和职责信息真实准确。供应商人员还必须披露之前在花旗或其任何前身公司（包括但不限于：花旗银行、花旗集团、Travelers、Salomon Brothers 和/或 Smith Barney）担任顾问或临时工的任何过往工作经历或派遣经历。

15.6 教育经历

供应商必须核实其人员已完成的最高学历。须核实的信息包括入学日期、教育机构名称、地址以及获得的学位。

15.7 犯罪背景

在法律允许的情况下，供应商的人员和分包商必须向花旗披露其是否因任何犯罪行为成为逮捕、传唤、传讯、提讯、起诉或定罪的当事人，包括认罪答辩或不抗辩以及参与任何审前转处或类似的程序。在法律允许且适用的情况下，对犯罪记录和/或指纹验证的行政审查必须在供应商人员开始执行任务之日前完成。对于和盗窃、诈骗、欺诈或背信有

关的犯罪行为（或当地法律采用不同定义的类似犯罪行为）的刑事定罪，除非法律另行禁止，否则可导致其无法获得花旗任务安排和/或不具备执行花旗任务的资格。根据适用的当地法律和法规，其他定罪记录可能导致其无法获得任务安排和/或不具备执行任务的资格。

15.8 重新筛查

被终止任命的供应商员工如被重新指派至花旗，则其必须接受重新筛查。如需了解有关重新筛查要求的更多信息，请参阅

https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf。

15.9 国际调动

所有筛查必须遵守任务执行所在国家的法规。如供应商人员转调至另一个国家，则须根据该国规定对相关个人进行重新筛查。

16 费用

按合同规定有资格要求报销业务费用的供应商。

16.1 概览

花旗仅会报销满足下列条件的合理业务相关费用：已获得花旗事先书面批准；属于供应商产生的与向花旗提供产品和服务有关的费用；符合适用合同的条款或花旗的 **Operating Expense Governance Policy** 及其相关标准和程序（如适用）；可通过支持性收据、发票、行程或花旗认为可以接受的其他形式的文件得到充分证实。

16.2 报销

此类费用须根据花旗的发票开具要求予以妥善记录并向花旗开具发票。花旗员工不得代表供应商产生供应商费用。任何提交给花旗报销的有效且已获批的费用项目，除满足所有其他发票要求外，还必须包含以下内容：

1. 费用的业务目的；
2. 费用金额和说明；
3. 费用地点和日期；
4. 供应商所提供服务的项目名称/说明；
5. 申请产生费用的相关服务的花旗代表姓名及其业务关系；以及
6. 采购订单编号（如适用）。

有关允许的可报销业务费用的信息，请联系您的主要花旗业务联系人。支持性收据、发票、行程或花旗认为可以接受的其他形式的文件必须与报销申请一起提交。报销申请必

须符合适用合同或花旗的 **Operating Expense Governance Policy** 及其相关标准和程序（如适用）的规定，并由相应的业务发起人和/或花旗主要业务联系人批准，以及由获得正式授权且有足够金额购买相应商品的人员批准。不合规的申请将不予报销。

17 信息安全（IS）

适用于以下供应商：访问、处理、存储或管理附录中分类和定义的任何花旗信息；或托管面向互联网的花旗品牌应用程序；或连接到花旗网络资源；或需要在无人陪同的情况下进入花旗设施。

17.1 概览

本节规定了在信息保护控制方面对花旗供应商（包括存储、处理、管理或访问花旗信息或托管花旗应用程序的供应商子处理商或分包商）或与花旗有网络连接的供应商的最低要求。这些要求确保按照适用的法律和法规要求以及花旗与其供应商业务开展地点的最高行业标准（例如 **ISO/IEC 27001/2**）对信息加以保护。如果当地法律、法规或相关行业标准的要求高于本节规定，供应商须遵守此类法律、法规或标准。此外，供应商可能还需要将额外的信息安全实践和程序纳入其合规范围，以遵守花旗的其他政策和合同条款。如果供应商决定针对信息安全实施其他安全实践或程序，则须确保此类实践和程序不与本节规定的最低控制措施相冲突。

17.2 信息安全政策与治理

供应商必须制定书面的信息安全政策和标准。政策治理必须包含明确定义的角色和职责，并进行年度政策和标准审查/更新，以符合当前的技术状态、行业标准、法律和监管要求。

17.3 职责分离

供应商必须设置流程，以确保任何人员均无法同时兼任两种业务职能、IT 职能或受控信息系统职能，并且无法在未经授权或未被察觉的情况下持续访问相同的活动、变更、信息系统或交易，除非有充分的补偿性控制措施降低这种风险。

表 A

职能	职能说明
开发/工程	设计、创建或修改软件、硬件和配置；示例可能包括： - 设计和创建新的应用程序代码和相关数据库架构 - 设计基础设施产品和应用组件 - 定制技术产品以集成至软件和服务
审批	批准代码变更的上线实施
系统实施/管理	安装、部署或管理软件、硬件和配置变更。示例可能包括：

	- 向生产环境基础设施执行自动化或手动代码发布 - 安装技术产品或设备 - 启动或停止服务，以支持涉及生产数据的系统故障排除和修复
审查特权 ID 活动	验证变更管理活动或安全相关系统事件（例如审计追踪）
管理 ID	添加、修改和删除 ID（用户、FID 和机器人）、权限或密码
业务职能	职能说明
发起业务交易	发起（也称为输入、创建）业务交易并更改客户信息
审批业务交易	审批（也称为授权、核对或放行）业务交易
IT 职能	职能说明
网络运营	对提供网络基础设施服务的产品进行设备管理与运维支持。例如：网络路由器、交换机、防火墙及域名服务（DNS）
非网络运营	对不提供网络基础设施服务的产品进行设备管理和运维支持。例如：服务器、电话及计算机

17.4 管理层对信息安全的承诺

托管花旗品牌面向互联网的应用程序和/或有权访问归类为机密或更高级别的花旗信息的供应商，须遵守花旗的第三方信息安全评估流程（TPISA），此流程会针对与信息安全相关的花旗要求以及（适用于花旗或供应商的）任何法律及/或监管要求的遵守情况对供应商政策、程序和控制措施进行评估。

该评估包括要求供应商回答并提供支持证据的安全问卷调查，还可能包括对第三方存储、处理、管理或访问花旗机密或更高级别信息的供应商地点的实地考察。此外，TPISA 第三方持续监控团队可使用网络安全监控工具对供应商进行监控，这些工具利用公开获得的信息来识别易受攻击的面向互联网的系统、主机、应用程序和服务，以应对报废软件、被利用的开放端口、漏洞或其他危害。如果 TPISA 的调查结果披露或表明存在安全缺陷，花旗会向供应商书面通知调查结果，并与供应商合作确定消除此类缺陷的方法。供应商必须及时采取必要的纠正措施和/或补偿性控制措施，以解决花旗自行判断的关注事项，并满足花旗根据问题风险等级确定的时限要求：高风险问题为 180 个日历日，中风险问题为 240 个日历日，低风险问题应在下一合规日期之前解决。

1. 供应商必须依照自己的信息安全标准、政策和程序，定期对其业务经营及相关控制措施进行评估。定期评估必须至少包括：
 - a) 评估供应商使用的流程，确保符合供应商自己的 IS 政策和标准；
 - b) 评估辅助资源，例如供应商使用的应用程序和基础设施，以及供应商分包商（如适用）为支持业务经营使用的 IS 流程，或者允许花旗执行

此类评估。如果第三方与访问、处理、管理或处置被花旗归类为机密或更高级别花旗信息的外包商签订新合同或续签现有合同，则须遵守相关规定。

2. 任何信息安全风险评估（例如 **TPISA**）中发现的问题均须记录在案并跟踪直至解决，同时向花旗提供补救措施的证据。
3. 如果供应商的信息安全管理职能部门被迁往境外，则在进行此类搬迁前，供应商必须获得花旗的书面批准。
4. 如果供应商收购了新的实体，则供应商必须对所收购的实体开展评估，以确保其符合这些标准。
5. 除非事先获得花旗书面批准，否则供应商不得外包安全管理职能，包括但不限于：针对用于存储、处理和/或传输花旗信息的系统的防火墙管理、安全配置管理、补丁管理或信息安全管理（**ISA**）职能。
6. 如果供应商托管包含花旗信息或者带有花旗品牌标记的软件或网站，则须按照花旗 **System Security Testing Standard (SSTS)** 定期对软件或网站进行漏洞评估，并在该标准规定的时限内纠正评估过程中发现的任何重大问题。由于 **SSTS** 未获批准进行外部分发，供应商必须与其花旗关系经理合作，以确保遵守参考文献。此外，供应商还必须遵守 **ISO/IEC 27001** 信息安全管理标准（或制定更高标准和协议的后继信息安全管理标准），并遵守本节（**17**）所包含的信息安全规定。
7. 如果需要连接花旗内部网络上的服务器和/或信息系统，则供应商必须通知其主要的花旗业务联系人，以便遵循现行的连接配置流程。
8. 如果花旗信息在未经授权的情况下被访问、获取，或者花旗信息丢失、损坏或被删除，或者用于存储、处理和/或传输花旗信息的信息系统受到任何其他损害，供应商必须及时通知相关的花旗联系人（业务活动负责人[**BAO**]）。
9. 供应商必须确保对所有高风险活动或敏感数据的更改进行审核追踪，以便明确此类操作的执行者。
10. 供应商必须确保在屏幕和书面文件（例如，包括监控、例外情况和监管报告以及其他报告）上屏蔽机密或更高级别的数据。
11. 供应商必须限制打印、记录或复制敏感数据，包括通过其自带设备。在协议期间或协议结束时，供应商须在约定的时间点归还或销毁所有花旗信息，除非法律或法规另有禁止。
12. 供应商必须确保所有能够访问花旗信息的供应商人员（员工、承包商、临时工、分包商）签署不披露或保密协议。
13. 必须向供应商的员工提供员工手册或类似文件，其中包含对违反供应商行为守则和人力资源政策的不合规行为进行纪律处分的流程，这些流程必须作为其入职流程的一部分让其知悉。
14. 供应商已制定相应流程，确保在员工或非员工被解雇或辞职时收回所有资产。
15. 如果任何机密信息在网站或网络访问系统上进行维护或以任何方式存储在那里，则供应商必须向花旗披露此信息。可将该披露包含在服务的说明中。如果供应商维护或存储花旗机密信息，供应商将在本协议期限内每年执行一次 **SSAE 18** 审计（或花旗批准的任何后续权威评估），并将至少每年向花旗提供一次记录此类 **SSAE 18** 审计结果或花旗批准的任何后续权威评估结果的报告副本。

16. 如果供应商在任何合并、收购或类似交易中被收购，或收购另一家实体，且此类交易可能影响服务，则供应商必须及时以书面形式通知花旗，并且必须按照本要求对由此产生的实体进行信息安全评估，以确保该收购或合并不会影响其遵守本要求。

17.5 分包商信息安全风险

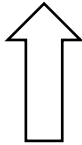
供应商必须要求能够访问花旗机密或更高级别数据的分包商由合格的信息安全人员在合同签署前以及合同签署后定期进行信息安全（IS）评估。此类评估应按照管理层批准的流程进行，该流程涉及评估流程从启动到问题管理的所有阶段。分包商 IS 评估应使用问卷或同等工具，评估分包商在与花旗第三方 IS 评估问卷（TPAQ）所涵盖领域一致的 IS 领域中的安全状况，并应包含用于计算与使用该分包商相关的 IS 风险的逻辑方法。供应商必须跟踪评估完成情况并管理注意到的问题和纠正措施计划，直至问题得到解决。

17.6 资产责任

- 1. 供应商须确保维护一份清单，列明其控制下用于存储、处理和/或传输花旗信息的所有应用程序和硬件。
- 2. 供应商须确保根据适当流程，对在其控制下的花旗信息资产进行清点，并持续维护该清单的准确性和完整性。
- 3. 供应商须负责保护其控制下的所有花旗信息。
- 4. 供应商须确保以符合行业惯例的方式实现其用户活动的可追溯性。
- 5. 必须限制用户从存放花旗信息的供应商全球网络访问个人外部互联网电子邮件存储和云存储账户。

17.7 信息分类与处理

花旗根据以下信息分类表对信息进行分类。请参阅附录，了解以下列出的各项信息类别的定义和示例。

受限	最敏感
敏感 PII	
机密 PII	
机密	
内部 PII	
内部	
公开	最不敏感

- 1. 花旗必须与供应商一起根据花旗信息分类指定信息保护所需的安全级别，且如果花旗需要提高或修改级别，供应商须确保制定充分的控制措施。
- 2. 如果内部或更高级别信息须存储在第三方管理的设备上，则这些设备必须受第三方与花旗之间合同的约束，并且该合同中包含符合花旗政策和标准的保密条款。
- 3. 如果供应商允许使用非公司所有的设备（即由第四方管理的设备）存储花旗数据，供应商必须制定相应政策，要求获得特定管理层的批准，并且为花旗信息的使用和处置制定指导方针和监控程序。
- 4. 供应商必须始终保护花旗信息免遭未经授权的访问、修改或删除。

5. 通过电子可传输介质（ETM）传输的归类为“机密”或更高级别的花旗信息，必须使用经批准的加密算法进行加密，并且必须确认送达。供应商必须确认 ETM 已送达至指定接收方。如果截至预计送达日期仍未收到接收确认，供应商必须通知花旗。

17.8 安全配置

1. 供应商必须为所有可能存储、处理、访问或传输花旗信息的资产保持文档化的安全配置标准。
2. 供应商须将信息安全控制措施纳入其选择、开发和实施应用程序、产品及服务的流程和程序。
3. 供应商必须为存储、处理和/或传输花旗信息的所有系统建立安全构建流程。
4. 供应商必须为所有系统维护安全的系统镜像或模板。
5. 所有默认用户账户和密码必须从供应商支持的系统、网络设备和应用程序中移除和/或更改。
6. 任何已被入侵的系统或服务均须使用经过完整性验证的镜像或模板进行重建和配置。
7. 对安全配置所做的任何更改均须通过供应商的变更管理流程获得管理层的批准。
8. 供应商必须将安全配置的任何更改通知花旗。
9. 安全构建流程必须包含相关工具，以支持在生产部署时对安全配置/标准构建设置进行自动化配置检查，并持续监控是否符合基线配置要求以及是否存在偏离基线配置的情况。

17.9 加密要求

供应商不得以未加密的方式传输机密或更高级别的信息。归类为“机密”或更高级别的信息必须使用花旗批准的工具或解决方案进行端到端加密。用于数据加密传输的批准协议及其相应版本号如下：

1. 交换身份验证和授权信息时：SAML v2.0、OAuth v2.0（仅限授权），
2. 为保护通信通道和关联的密钥交换，只允许使用以下网络安全协议：
 - a) 首选 TLS v1.3，所有 TLS v1.3 套件均允许使用。如果 TLS v1.3 是唯一启用的协议，则无需进行额外审查。
 - b) 如果 TLS v1.3 在技术上不可行，而使用 TLS 1.2，则 SSL Labs 评级为 B 或更高即可接受，无需进行额外审查。

在花旗第三方环境中持久存储的数据必须采用花旗认可的工具或解决方案进行完全加密；交换这些数据时亦需如此。用于数据加密的批准算法和密钥长度如下：

1. **Advanced Encryption Standard (AES)**：批准的密钥长度：256 位或更高。
受限模式：禁止使用电子密码本（ECB）模式，除非明文数据量小于或等于分组长度。磁盘驱动器加密：要求使用采用 256 位密钥的 AES。AES 128 位密钥长度可作为 TLS 密码套件选项使用；但是，为支持花旗与国际时间计划

保持一致（参考 NIST 8547 IPD），自 2028 年 12 月 31 日起，将不再允许使用此类配置，并将统一采用 256 位或更高强度的密钥。

2. **ChaCha20**（用于关联用例的流密码）：批准的密钥长度：128 位或 256 位，随机数为 96 位，分组计数为 32 位；或者随机数为 64 位，分组计数为 64 位。最大数据大小：16 PB。

认可的公钥密码系统、密钥交换、协商机制、消息摘要和密钥派生函数如下：

有关供应商量子就绪状态的通知：供应商必须通过（[调查链接](#)）向花旗量子就绪项目团队提交其关于 NIST IR 8547（公开初稿）的表 2 和表 4 覆盖范围的计划。

1. **公钥密码系统和最小密钥长度：**
 - a) Rivest–Shamir–Adleman（RSA）：2048 位。
 - b) 数字签名算法（DSA）：2048 位。DSA 不得用于保护在花旗以外处理或存储的花旗数据。
 - c) 椭圆曲线数字签名算法（ECDSA）：256 位，符合 ANSI X9.62 中的规定，具有 NIST 推荐曲线。
2. **密钥交换和协议机制及最小密钥长度：**
 - a) Diffie-Hellman（DH）/临时 Diffie-Hellman（DHE）：2048 位。
 - b) 椭圆曲线 Diffie-Hellman（ECDH）/临时椭圆曲线 Diffie-Hellman（ECDHE）：256 位，符合 ANSI X9.63 中的规定，具有 NIST 推荐曲线¹。
3. **消息摘要功能：**禁止创建长度大于用于生成哈希值的随机数据比特数的加密密钥。
 - a) SHA-1 仅可用于非数字签名应用。SHA-2 系列、SHA-3 系列和 POLY-1305：可用于所有加密哈希函数应用。
4. **基于密码的密钥派生函数及最低要求：**
 - a) PBKDF2：最小迭代次数为 10000，盐值至少为 16 字节。
 - b) HKDF：必须使用盐值，并且必须包含信息输入值。
 - c) SCRYPT：最小轮数/成本因子至少为 10。
 - d) 禁止采用 NIST SP800-108 KDF 进行流加密。NIST SP 800-108 KDF 模式，即计数器模式、反馈模式和双管道迭代模式，均可接受。
 - e) 建议使用 Argon2。
5. **密码哈希函数和最低要求：**
 - a) Bcrypt（用于身份验证资料的本地存储）：最小轮数/成本因子至少为 10。
 - b) 在任何已部署供应商产品的环境或系统上本地存储密码时，建议使用 Argon2 或 PBKDF2 进行密码哈希运算。

17.10 外部电子邮件

根据规定和/或供应商政策，在供应商不得使用花旗认可的端到端加密软件或工具的情况下，对于包含花旗信息类别为机密或更高级别的花旗信息的个人电子邮件，通过传输加

¹ ECDHE 是首选。

密（例如通过传输层安全协议[TLS]进行的网关到网关加密）可完全满足加密要求。批准的安全电子邮件协议为：

1. **身份加密（IBE）** 具有加密电子邮件功能，只能在花旗面向客户的解决方案以及安全电子邮件和电子交付系统内使用。
2. **强制性 TLS（MTLS）** 具有会话加密功能（不加密电子邮件有效载荷），可用于已预先协商使用协议的供应商、合作伙伴和客户。
3. **域密钥识别邮件（DKIM）** 具有来源身份验证和密钥管理功能，可用于供应商、合作伙伴和客户。

17.11 专用网络

如果专用网络由认可的机构独立监管，且符合针对许可或认可的交易对手之间交易业务的金融行业标准（例如环球银行金融电信协会[SWIFT]或中央银行），则在这些网络提供必要的基础设施以完全支持加密传输之前，其可免受机密 PII 传输中加密要求的限制。

17.12 语音和传真

归类为“机密”或更高级别的花旗信息，通过传真发送或在语音通话（包括基于 IP 的语音通话[VOIP]）中讨论时，可以不进行加密。如有必要，供应商须制定具体流程和指南，以保护通过此类渠道传输的机密或更高级别信息。

17.13 加密密钥和证书管理

本节使用的安全边界一词是指加密模块验证计划（CMVP），如联邦信息保护标准（FIPS）、已验证边界（FIPS 140-2/3 2 级是可接受的最低安全级别）。（AWS Nitro Enclaves 等机密计算区可以接受。其他唯一安全边界案例必须得到花旗的批准。）

1. 供应商必须部署用于加密和签名（包括 SSH 密钥）的行业现行标准加密算法和最低密钥长度。当此类算法和密钥长度更新以符合行业标准时，供应商必须通过其变更管理流程提供保证。
2. 供应商必须制定正式的文档化密钥、机密和证书管理生命周期流程，并采取适当的控制措施来避免敏感资料被人擅自使用或泄露。所有加密密钥材料及密钥生命周期事件均须仅在安全边界内进行。必须记录对特权和安全边界的所有访问。供应商必须为所有密钥生命周期事件提供序列图，重点说明所涉及参与者、实体和边界。
3. 加密密钥必须具有唯一用途，不得用于任何其他用途。例如，不得将同一加密密钥同时用于磁盘加密和数据加密，也不得将同一加密密钥同时用于有效载荷加密和数据库加密。默认情况下，禁止 SaaS 供应商在多个租户之间重复使用加密密钥。只有在非关键、低风险的使用场景，且所涉及的花旗信息不属于机密 PII、敏感 PII 或受限级别时，方可在获得安全架构委员会明确批准的前提下例外允许。
4. 对于所有加密密钥（对称或不对称），私钥或私钥资料（如种子或私钥的一部分）在任何情况下都不得以明文显示。私钥或私钥资料（如种子或私钥的一部分）切不可离开安全边界，动态会话密钥等临时密钥除外。如果设计需要在安全区/特权访问边界之间传输对称密钥或者私钥或私钥资料，则只能使用对称密钥包装密钥或公钥传输密钥，通过相互 TLS 加密隧道以加密形式传

输，且此类传输必须得到花旗的书面批准。私钥传输密钥切不可离开在这些情况下生成密钥时所在的特权访问安全边界。

5. 对称密钥包装密钥必须拆分为两个或以上密钥组件并在分发之前进行异或运算，以便手动输入/加载。对称密钥包装密钥必须具有在 **CMVP** 验证模块等安全边界内关联的充分访问控制列表（**ACL**），并且对称密钥包装密钥不得存储在安全边界之外。
6. 人类、服务或自动代理对包含私钥、机密或私钥资料（如种子或私钥的一部分）的密钥库或安全边界的访问权限必须通过仅限授权人员或系统访问的控制措施进行妥善隔离。
7. 出于审核目的，每个访问包含私钥或对称密钥的密钥库的请求都必须加以记录，注明访问者、访问时间和访问目的等详细信息。
8. 供应商不得使用自签名、通配符证书或默认 **SSL** 证书。
9. 所有加密密钥必须具有明确的密码周期时段数据，如 **NIST SP800-57** 第 1 部分修订版 6 中所建议的那样。密钥在到期前必须定期更新或轮换，以考虑到变更周期、安排冲突和系统冻结。
 - a) 在更换过期证书时，禁止重复使用旧的不对称密钥对。
10. 一旦密钥的完整性、存储或共享密钥的介质，或者对称密钥或私钥的保密性疑似遭到破坏，则必须按照加密密钥泄露的情况进行处理。所有泄露的密钥必须从操作使用中删除，所有相应的证书必须予以撤销。
11. 必须使用行业标准加密算法对无线网络进行加密。
12. 无论采用何种形式的加密机制，供应商均须使用行业标准密钥管理工具和技术。密钥管理角色必须与运营管理隔离。
13. 供应商仅可在确保与花旗数据安全服务提供的 **PKI** 和 **KMS** 实现互操作，并且密码控制权未委托至花旗密码治理体系之外的情况下，使用云原生 **KMS** 和 **PKI**。

17.14 访问控制责任

为了保护用于存储、访问、管理、处理或传输花旗机密或更高级别信息的所有受控信息系统免遭未经授权的访问，供应商有责任实施最小特权原则，即将用户权限限制为每个工作职能所需的最低访问级别，并管理对所有系统和应用程序的逻辑访问权限的配置。控制措施必须予以全面记录且可审计。访问权限的开通与撤销（包括密码重置和账户启用）应尽可能通过自动化流程完成，以降低因人工操作失误导致权限过度授予等风险，并符合行业标准。

1. 供应商负责管理其组织内所有用户的访问权限。
2. 供应商必须实施访问控制，确保仅向用户授予履行其职责所必需的最低权限和访问授权。
3. 供应商必须建立相应流程，确保所有默认访问功能均已移除、禁用或受到适当保护，以防止未经授权的使用。

17.15 用户访问管理

供应商必须管理对处理、存储和/或传输花旗机密或更高级别信息的系统和应用程序的逻辑访问权限的配置。其中包括：

1. 已批准身份验证系统的标识和清单。
2. 必须规定，任何对花旗数据的访问均须获得经理（或其指定人员）以及系统所有者的批准。供应商负责确保其任何有权访问花旗数据的人员，仅依据按需知悉原则获得相应访问权限。
3. 必须规定，如向个人用户授予某种权限或功能组合会导致利益冲突或违反经办人与复核人分离规则，则不得授予此类权限或功能组合。
4. 监控流程，用于监督和管理为系统上每个用户所授予/所撤销的访问权限。
5. 访问权限申请不得基于镜像/复制其他用户的访问授权。所有申请必须明确指定所需角色和访问授权，并提供业务必要性说明，以防止权限逐步扩张，并确保遵循最小权限原则。

17.16 用户身份识别和验证

所有由供应商控制的信息系统必须在建立会话或启动可能访问花旗信息的交易之前，对访问这些平台的用户或系统身份进行认证。

1. 用户必须通过用户 ID 在技术平台中进行唯一标识或关联映射。
2. 用户必须使用经批准的身份验证方法向技术平台进行身份验证——供应商应联系其主要业务联系人（BAO），了解现有的已批准方法。
3. 必须根据花旗身份验证要求使用共享身份验证基础设施（例如单一登录、缩减登录及其他共享身份验证服务）；供应商应联系其主要 BAO，了解现有的已批准方法。
4. 用于向信息系统验证用户身份的身份验证数据（IVD）在传输和存储时必须加密。请参阅第 17.9 节，了解加密要求。
5. 供应商人员用于访问花旗系统的每个账户，必须关联至由花旗分配的唯一标识符（例如 GEID）。为确保操作可追溯、SOD 控制有效执行并满足审计要求，禁止人类用户使用通用账户或共享用户 ID。

17.17 特权访问身份识别和临时特权访问

供应商必须维护所有身份清单，并识别其中具有特权访问权限的身份，或可访问包含机密 PII 或更高级别信息的电子存储库（即支持业务应用的数据集或数据库）的身份。供应商必须实施控制措施，防范未经授权使用此类身份。如果员工要求访问特权 ID 或访问之前提到的电子存储库，则供应商必须通过符合以下要求的临时访问管理流程授予访问权限：

1. 要求申请人位列预先批准的授权用户名单上或在使用时获得批准。
2. 要求在授予访问权限前在变更/问题票据中提供正当理由并记录在案。
3. 包括对使用该访问权限所执行活动的独立审查。

4. 包括在临时访问发布期间结束时启动撤销/删除访问权限的流程。
5. 允许将生产环境和实施后稳定阶段的访问权限（例如在重大升级或故障修复后）延长最多七（7）个日历日。

17.18 用户访问权限审查

1. 供应商必须建立并记录相关流程，至少每半年一次，对用于存储、处理、管理和/或传输花旗信息的受控信息系统中的用户访问授权进行审查、验证，并删除不必要的用户访问授权。
2. 用户不得审查或批准其自身的访问授权，也不得审查或批准将审查职责委托给该用户的人员的访问授权。
3. 供应商员工在花旗内部发生职能变更后，供应商必须在 14 个日历日内完成访问权限和访问授权审查，并在员工的新职能不再需要访问花旗数据时移除相关访问权限。

17.19 安全登录程序

1. 被锁定的用户登录 ID 必须通过符合行业标准的重置服务或其他经授权的功能重新启用。当操作系统或应用程序支持时，所有网络入口点在用户首次登录或进行身份认证时必须显示横幅提示文本。

17.20 密码管理系统

1. 用户静态密码不得以明文形式显示在屏幕上。密码可见性切换功能可作为例外，但必须满足以下条件：
 - （1）密码输入默认采用掩码显示；
 - （2）密码可见性只能由用户执行明确操作后启用；
 - （3）用户停止相关操作后，密码必须在最多 15 秒内自动恢复为掩码显示。
2. 特权功能 ID 密码不得以明文形式进行硬编码。
3. 静态密码须至少包含十（10）个字符，其中须包含字母和数字，并区分大小写。静态密码的大小写区分功能必须在每个身份验证点进行验证。对于 2026 年 8 月 31 日之后上线的应用程序，功能 ID（FID）的静态密码长度必须至少为 15 个字符。
4. PIN 仅可在为满足物理设备限制（例如键盘、电话、智能卡）的必要情况下，作为访问信息系统的唯一身份认证方式使用。
5. 所有静态密码须至少每 90 个日历日更改一次。
6. 所有静态密码必须在最多连续六（6）次登录尝试失败或六（6）次连续密码重置尝试后锁定。密码必须通过身份管理员功能解锁，或在至少 30 分钟后自动解锁。
7. 所有身份认证系统必须实施登录不活动/未使用控制机制，且期限不得超过 100 个日历日。如技术可行，被禁用的登录账户可由用户本人或其他经授权功能重新启用。
8. 身份认证流程必须确保同一密码不得在最近六（6）次密码变更中重复使用。

17.21 系统实用程序的使用

供应商必须确保对能够改写系统和应用程序控制的实用程序的使用（例如通过外围设备启动）加以限制和控制。

17.22 会话超时

1. 用于存储、处理和/或传输花旗信息的受控信息系统的所有用户均须登录并重新验证身份。
2. 一段时间（不超过 30 分钟）内无活动，用户必须重新验证身份。活动包括对终端设备的任何输入操作（包括鼠标、键盘、触摸屏等）。如果密码保护的屏幕保护程序已实现该强制控制，则无需实施应用程序/单点登录强制控制。

17.23 终止用户访问

1. 员工被解雇或辞职后，可能允许访问花旗机密或更高级别数据的用户权限（包括桌面/Active Directory 用户登录名、单点登录[SSO]、电子邮件、一次性密码[OTP]令牌和远程访问）必须立即予以删除。
2. 如果员工有权访问花旗拥有和管理的系统，则在该员工发生职能变更或解雇时，相关人员必须立即通知花旗业务关系经理、BAO 或 BAO 支持，以确保花旗业务经理在其解雇日期结束前发起请求以删除被解雇员工的访问权限。
3. 供应商已制定记录在案的流程，以在员工或非员工被解雇或辞职时，根据第 17.23.2 节规定的时限，撤销其对所有资产的访问权限。
4. 如果供应商发现任何涉及 17.23.1-17.23.3 的异常，供应商必须立即通知花旗业务关系经理、BAO 或 BAO 支持，同时给出合理的理由并配置相应的控制措施。

17.24 远程访问

供应商必须制定远程访问控制措施，以保护对可能存储、处理或传输花旗机密或更高级别数据的网络的访问，其中包括：

1. 必须对存储、处理、管理和/或传输花旗信息的信息系统的远程访问加以保护，以防未经授权而遭使用。
2. 如果供应商管理的用于存储、处理和/或传输花旗信息的所有笔记本电脑和台式机在本地存储/处理花旗类别为机密或更高级别的信息时使用远程访问，则其均须使用符合行业标准的加密工具加密。
3. 只能通过采用多因素身份验证（MFA）的已批准远程访问解决方案建立远程连接。
4. 供应商管理的机器直接连于互联网时（即，不是通过供应商管理的防火墙或代理服务连接），须启用个人防火墙。
5. 供应商管理的设备必须定期接入供应商网络，以接收和安装软件/防病毒工具的定期更新，满足获得网络完整访问权限的要求。对于明确的设备更新目的，可以允许有限的访问权限。
6. 如果使用非供应商所有和管理的设备访问花旗机密或更高级别的信息，这些设备必须配置为使用不允许下载到本地设备的授权解决方案。必须制定以下控制措施：

- a) 防止花旗数据被下载到公司管理的解决方案之外的设备上。
 - b) 供应商必须确保此类访问由采用标准远程访问技术（例如虚拟桌面接口[VDI]）的令牌型或证书型身份验证方法提供安全保障。
 - c) 远程访问解决方案（如终端服务和 VMware Horizon）必须配置为禁用基于 Blast、PCoIP 协议的剪贴板共享和驱动器映射，以及禁用 RDP 和 SSH 协议。
7. 如果将软令牌用于 MFA，例如访问移动设备上的软件应用程序，则软令牌身份验证软件必须对用户进行身份验证（例如通过密码、生物特征等），如果手机已越狱或获得超级管理员权限（使用并非由移动设备供应商认证和提供的操作系统），则应避免使用软令牌。
8. 按照这些要求，需要对直接或间接与为花旗提供的服务有关的系统、数据存储库、应用程序和/或基础设施拥有特殊、特权和/或管理级别的访问权限（包括但不限于系统管理员、数据库管理员、访问控制管理员、防火墙管理员、网站管理员等）的所有供应商人员（包括但不限于固定/临时员工、承包商和分包商）必须只能通过 MFA 进行身份验证，且此类访问权限应由供应商进行独立记录和监控，以防范可疑活动和/或未经授权的访问。
9. 对于个人拥有的设备和第三方拥有的设备，供应商必须制定有效解决方案，确保此类设备具有经批准的操作系统版本、补丁级别、防病毒和防恶意软件解决方案，然后才允许此类设备登录到网络。
10. 供应商必须确保其所有人员：
- a) 保持一个私密、专用的远程工作区，未配备任何语音辅助设备（例如 Siri、Alexa）、视频录制设备和/或任何其他照片、视频或音频播放/拍摄录制设备。未经授权的人员不得查看可能出现在远程计算系统屏幕上的任何数据、系统、应用程序。
 - b) 设备处于无人值守状态时应锁定计算设备，以充分降低未经授权查看屏幕内容的风险。

17.25 桌面清理政策

供应商人员必须保护所有形式的花旗信息，包括在工作场使用或存储的物理信息。供应商须至少每年通过 IS 培训或其他渠道向全体员工传达此要求。

17.26 消防安全

- 1. 供应商必须遵守有关实体安全和建立安全工作环境的适用法律法规要求，包括当地消防规范。
- 2. 供应商必须使用火灾探测、报警和灭火系统。系统必须每半年检查一次，每年测试一次。

17.27 物理安全

- 1. 花旗信息必须存储在仅限获授权人士访问的安全区域。
- 2. 供应商必须设置记录在案、可予审计的物理访问控制系统。
- 3. 供应商必须根据其运营环境及所提供服务的状况，采用适当的综合安全防护措施，包括由第三方监控的安全报警系统、安全警卫和视频监控系統。

4. 供应商须有记录在案的访客政策，包括要求所有访客在抵达、签入和签出时提供可验证的身份信息。

17.28 运营安全程序和责任

1. 供应商变更管理流程必须包括有关变更的登记、审查、测试、批准、实施和关闭的关键检查点控制措施。供应商还必须建立紧急变更流程，该流程必须要求执行上述所有阶段，包括强制性审批层级。
2. 供应商必须围绕容量管理制定可审计的流程，其中包括（但不限于）可用性、容量和绩效度量标准/指标；业务影响评估；主动跟踪、调查及解决绩效和容量问题。
3. 供应商须酌情确保实验室、开发、测试和生产环境在物理和/或逻辑上进行完全的分离。

17.29 软件开发要求

适用于为花旗专门开发软件的供应商。供应商必须遵循本节要求，或提供已形成文件并经批准的软件开发生命周期（SDLC）流程，该流程应采用与本要求具有同等质量和效果的等效方法。

17.30 启动和规划

供应商必须按照花旗的要求和合同义务定义解决方案的范围和目标。其中包括：

1. 记录功能性和非功能性需求；
2. 提供工作量和时间安排估算；以及
3. 确定所有第三方组成部分或依赖关系。

包括安全风险评估在内的合规活动必须从项目启动阶段开始执行。必须明确传达各相关角色、职责及审批节点。

所有环境必须划分为开发环境（DEV）、测试环境（TEST）或生产环境（PROD），并在整个软件生命周期内保持严格隔离。环境分类决定访问权限以及可处理的数据类型。供应商必须依据环境分类限制访问权限，并确保部署符合相应 SDLC 阶段完成要求，以防止未经授权的访问或数据泄露。

17.31 设计

供应商必须记录设计方法，以确保交付解决方案满足所有已声明的需求（“测试计划”）。测试计划至少应包括并说明：

1. 开发团队执行的所有测试，包括单元测试、功能性测试、非功能性测试以及性能相关测试，并建立测试与需求之间的可追溯关系；
2. 确认测试完成情况的审批人员；
3. 安全测试要求，包括漏洞评估和威胁建模；以及
4. 测试环境、测试方法、测试流程和发布路径。

供应商必须制定发布策略，明确发布至 TEST 和 PROD 环境所需的先决条件及流程，包括发布就绪标准、发布内容以及项目生命周期内的交付节奏。

如合同另有规定，软件分发包必须使用花旗批准的工具和工作流程，并按照花旗批准的格式进行打包。

17.32 测试

测试必须在受控环境中规划和执行，以验证解决方案符合规定的要求和成功标准。测试用例必须可追溯至需求和代码提交记录。

供应商应准备一份报告，总结测试通过/失败的结果、开发过程中执行的额外测试以及任何未完成的测试（并说明原因）（即“测试退出报告”）。缺陷和延迟实现的功能必须记录在案，同时还需制定未解决问题的缓解计划。

供应商必须应花旗的要求提供以下证据：

1. 详细的测试计划；
2. 测试退出报告中详细记录的测试完成情况及测试结果；以及
3. 测试结果与需求及代码提交记录之间的可追溯性证明。

17.33 部署

部署之前，供应商必须完成所有必要的安全测试，包括漏洞扫描和威胁建模。发布流程必须采用规范化管理，并包括有文件记录的变更记录、回滚策略以及所需的审批。实施计划和部署操作手册必须包括监控和上报规程。

部署后，供应商必须最终确定系统标识符并更新所有相关文档和工件，以确保做好审计准备。

17.34 安全

1. 在 SDLC 的设计阶段必须开展结构化评估，在代码编写前识别并解决潜在的安全风险、漏洞和架构弱点（“安全设计审查”）。该审查须纳入到 SDLC 中，并包含符合 OWASP 等行业标准的预防性及检测性控制措施。
2. 供应商必须遵循安全编码规范。
3. 供应商须将信息安全控制措施纳入其选择、开发和实施应用程序、产品及服务的流程和程序。
4. 供应商必须为存储、处理和/或传输花旗信息的所有系统制定安全构建程序，并且必须为所有系统维护安全映像或模板。

17.35 针对恶意软件的控制措施

供应商必须确保实施相应的控制措施，以防止和检测引入任何恶意代码（例如病毒、蠕虫、特洛伊木马病毒、广告软件、间谍软件、勒索软件或其他可能导致数据泄露的类似网络攻击）。供应商须：

1. 在所有个人计算机上采用、更新和维护反病毒和反间谍软件技术，在所有局域网（LAN）服务器、邮件服务器以及存储、处理和/或传输花旗信息的其他设备上采用、更新和维护反病毒和反间谍软件技术。
2. 部署安全设置，以防止最终用户禁用防病毒/防恶意软件工具和计划扫描。
3. 采用集中管理的自动化程序来配置和更新防病毒和防恶意程序软件。
4. 确保实施相关流程，以识别和处理防病毒签名或扫描引擎过时的不合规计算机。
5. 控制对用于连接外部设备（包括但不限于存储介质）的通信端口/接口的访问。

17.36 针对移动代码的控制措施

供应商必须确保围绕安全移动代码实践实施相应的控制措施。如果移动代码的使用获得授权，其配置至少须满足所有相关行业标准及对花旗负有的合同义务，供应商必须确保已授权的移动代码按照明确界定并记录在案的安全政策运行，并防止未授权的移动代码运行。

对于可能影响底层操作系统或平台的移动代码（即在“沙盒”以外），供应商须确保：

1. 供应商公布的移动代码须经花旗认可的证书颁发机构签署，证书的生命周期须由供应商管理（以处理证书过期或轮换问题）。
2. 证书过期的已签署移动代码须从生产环境中删除。

17.37 审计日志记录

供应商必须确保访问、存储、处理、管理和/或传输花旗数据的所有受控信息系统在基础设施或应用程序层面保留审计追踪，以记录以下各项：

1. 与相关平台有关的基础设施安全相关操作
2. 与防火墙或 IDS/IPS 生成的安全事件有关的所有系统警报
3. 所有试图违反系统安全的行为（例如用户登录尝试失败）
4. 所有未经授权访问资源（软件、数据、流程等）的尝试
5. 管理员操作
6. 与从用户或其他系统接收特定信息有关的信息
7. 与金融交易和花旗信息有关的所有重要事件，特别包括以下各项：
 - a. 金融交易更新
 - b. 机密或敏感 PII 数据更新
 - c. 受限数据更新
 - d. 身份验证数据更新
8. 所有已建立的会话
9. 在技术上可行的情况下，必须采集会话信息（例如唯一设备标识符），并将其记录在面向花旗的应用程序（即网站和移动应用程序）中，以支持欺诈调查。这些信息必须至少包含 IP 地址。必须采集花旗交易和花旗账户开立活动的会话信息。捕获的信息必须能使会话项目与交易或开户产生关联。
10. 审核追踪必须记录特定活动归属于特定个人的情况，以防推脱责任。
11. 必须记录重大信息安全管理（ISA）事件，尤其要记录以下各项：
 - a) 用户创建
 - b) 用户访问权限修改
 - c) 受控信息系统上的用户配置文件删除、创建和修改
 - d) 密码重置
 - e) 系统安全配置更改
 - f) 特权功能 ID 的所有交互活动
 - g) 不论生成日志的是哪种系统，安全日志必须至少包含以下信息，除非此类包含操作在技术上不可行：
 - i. 事件的日期和时间（UTC 格式时间）

- II. 执行该操作的个人的用户 ID
- III. 事件类型
- IV. 受影响的资产或资源名称
- V. 访问类型（删除、修改等）
- VI. 事件的成功或失败
- VII. 来源（终端、端口、位置、IP、主机名等）

17.38 日志信息保护

供应商必须确保实施访问控制措施，以便在启动、关闭、存储和传输期间保持审计追踪的完整性。

1. 为防止未经授权修改审核记录，供应商须确保其活动受到追踪的系统用户无法改写或修改记录。
2. 供应商必须向花旗提供日志数据记录保存程序，该程序应明确数据维护方式，并包含符合所有适用法律法规要求的合规措施。
3. 组织或安全域内所有相关信息处理系统的时钟，均须与准确的时间源保持同步。

17.39 监控系统使用情况

供应商必须确保直接或通过自动审核流程对以下事件进行捕获、记录和审核：

1. 与防火墙或入侵检测系统（IDS）/入侵预防系统（IPS）生成的安全事件有关的所有系统警报。
2. 安全标准内部版本中确认的所有关键资源更新。
3. 由任何能够访问归类为机密 PII 或更高级别信息的 ID（功能、特权、系统、临时等）执行的所有交互活动。
4. 上文审核记录部分列出的重大 ISA 事件，但下列情况除外：
 - a) 对于由具备端到端完整性控制措施的自动化工作流/履行系统执行的信息安全管理活动，从用户、角色或配置文件中移除权限。

17.40 日志关联和审核

1. 当记录的事件触发警报时，将对该事件进行审核，如果有迹象表明可能已发生潜在的有害信息安全事件，则供应商必须采取后续行动并进行调查。
2. 供应商必须确保审计日志汇总到一个安全信息和事件管理（SIEM）系统或日志分析工具之类的中央日志管理系统中，以进行日志关联分析和审核。
3. 供应商必须定期审核和调整其 SIEM 或日志分析工具的配置，以改进可操作事件的识别。

17.41 操作软件控制

供应商必须确保仅使用当前由行业认可的商业供应商提供支持，或者拥有可解决安全问题的有效和适当版本补丁及配置更新的操作系统和软件。

供应商必须确保实施有据可查的流程，明确规定所有已批准的安全补丁和配置的应用期限。

无论供应商与花旗之间是否另行签订维护协议，供应商均须确保，为花旗开发并受许可协议约束的软件不得使用存在已知漏洞的已停止支持的软件版本，并确保相关软件按照要求及时完成更新和补丁修复。

用于处理花旗信息的应用软件必须从经认可且信誉良好的供应商处获取，并且必须获得有效授权许可、纳入软件资产目录管理，并处于受支持状态。

17.42 漏洞和威胁管理

1. 供应商必须实施漏洞与威胁管理流程，该流程应全面涵盖和/或包括以下所有内容：
 - a. 用于发现和管理所有可用于处理、存储、访问或传输花旗机密或更敏感数据的资产中漏洞的工具和流程。
 - b. 要求至少每周使用行业认可的漏洞工具和报告方法进行扫描。
 - c. 必须依据最新版本的“通用漏洞评分系统（CVSS）”对漏洞进行分级，并根据漏洞严重程度制定相应的修复时间表。
 - d. 要求在全面生产部署之前测试漏洞补救情况。
 - e. 记录在案且可重复的加快补救关键漏洞操作流程。
 - f. 供应商必须在资产可支持生命周期内持续跟踪和管理资产，以提前准备应对生命周期终止（EOL）或供应商支持终止（EOVS）状态，并制定流程以主动升级或替换相关资产。
 - g. 通过情报收集、漏洞扫描或渗透测试发现的任何关键 CVSS 评分漏洞均须优先处理，并在与漏洞风险相称的明确时间范围内进行修复。

17.43 第三方托管应用程序

如果供应商在网站或可通过互联网访问的系统上维护或存储花旗机密或更敏感的数据，则为了防范涉及影响花旗的产品或服务的漏洞或威胁（每一项为一个“漏洞”），供应商必须遵守以下要求：

1. 指定一名供应商员工负责回复花旗有关信息安全的问询。
2. 利用行业公认的最佳实践，按不少于每周一次的频率定期监控计算机安全漏洞信息的可靠来源（如 FIRST、CERT/CC 和 CISA 已知被利用漏洞目录和供应商邮件列表），并采取适当措施获取、彻底测试、应用并向花旗提供相关服务包、补丁、升级和变通方案。
3. 至少每季度对信息安全措施的实施情况进行测试，测试方法包括使用网络、系统和应用程序漏洞扫描工具和/或渗透测试。
4. 允许花旗或花旗认可的第三方在合理的时间间隔内，采用商业可用工具和/或行业标准实践进行漏洞评估、道德黑客测试或其他安全评估，以验证供应商是否遵守任何合同及本要求所规定的义务，包括但不限于政策、流程和程序的审查，物理安全措施的现场评估，网络、系统和应用程序漏洞扫描以及渗透测试。
5. 任何为供应商提供漏洞评估服务的承包商均须来自花旗批准的漏洞评估供应商列表。如供应商委托承包商或分包商提供相关服务，供应商必须在自行承

担相关费用的情况下，确保任何所需的漏洞评估按照供应商直接提供该等服务时适用的同等时效要求完成。供应商还必须确保，要求任何承包商或分包商配合开展此类评估的义务，已在供应商与该承包商或分包商就相关服务签订的协议中予以明确约定，其中包括授权花旗开展此类评估的条款。

6. 通知

- a) 如果供应商发现涉及影响花旗的产品或服务的漏洞，则供应商必须在发现漏洞之后 24 小时内以书面形式通知花旗，并随附供应商所要采取的补救措施的说明。
- b) 如果供应商通过可靠的公开披露流程渠道（在国家漏洞数据库[NVD]中或通过提供给外部安全供应商的威胁目录发布漏洞）了解到涉及影响花旗的产品或服务的漏洞，则供应商应在此类发布之后 24 小时内以书面形式通知花旗。每份通知均应包含有关漏洞的信息、系统对花旗相关服务的用途（例如，系统是否托管花旗信息、是否用于提供服务或两者兼有）、漏洞是否可被远程利用；以及通用漏洞披露（CVE）评分。供应商将继续向花旗提供更新，直至漏洞得以修复。如果花旗发现漏洞，则花旗可就此向供应商发出通知，供应商应按照本节的要求及时修复漏洞。

7. 补救措施。对于根据本节规定提供的每一个漏洞，通知方将根据严重性以及给花旗带来的风险，对该漏洞的风险级别和影响予以评估，并根据附录中所述的通用漏洞评分系统（CVSS）分配风险优先级（见

<https://www.first.org/cvss>）。风险等级经分配并经各方达成一致之后，供应商应修复任何已发现的中、高风险等级的漏洞或关键漏洞。在可能的情况下，将在针对当前已部署版本的安全包中提供对任何漏洞的修复措施。

如果供应商无法或不愿按照令花旗满意的方式修复漏洞，则花旗有权终止适用的许可，且花旗无需承担任何进一步的责任或财务义务（对于终止部分）；供应商应立即向花旗退还已支付许可费用中按比例计算的相应部分。

17.44 通信安全网络控制措施

1. 供应商用于访问、存储、管理、处理和/或传输花旗信息的网络必须实施安全防护措施，以抵御威胁，并通过网络中的安全策略执行控制点确保相关信息系统的安全。

- a. 花旗信息归类为“机密”或更高级别的信息不得在面向互联网的 **DMZ** 系统中进行持久化存储。采用无线局域网（**WLAN**）或其他无线设备解决方案访问、存储、管理、处理和/或传输花旗信息的网络，如已部署合理的访问控制措施（例如 **PEAP-TLS**、**EAP-TTLS** 等）以防止未经授权访问，则可连接至包含花旗信息的网络。
 - b. 供应商全球网络的所有外部 **IP** 连接均须由供应商管理的防火墙提供保护。
 - c. 供应商应部署实时入侵检测系统（**IDS**）和入侵防御系统（**IPS**），以便监控并保护与用于访问、管理、存储、处理或传输花旗信息的供应商网络的互联网连接。
2. 对于所有花旗品牌的互联网应用程序，供应商必须确保：
- a. 在供应商网站上托管的服务均得到花旗认可的防护 **DDoS**（分布式拒绝服务）服务或花旗验证的同类控制措施的保护。
 - b. 必须为外部防火墙配置默认拒绝规则。防火墙规则必须根据最低特权原则进行配置，并且防火墙拒绝的所有连接尝试（例如丢包）都应进行日志记录/记录。
 - c. 网络通信流量在默认情况下应予以拒绝，但托管接口按例外情况处理，予以允许。例外情况必须严格限定在特定来源、目的地和服务。
 - d. 网络应用程序流量应具有适当的控制措施并经过过滤，例如通过 **Web** 应用防火墙进行防护。

17.45 网络隔离

供应商必须确保，所有用于访问、存储、处理、管理和/或传输花旗信息且可通过互联网访问的信息系统和应用程序仅能通过供应商的 **DMZ** 进行访问。

在紧急事件发生期间，供应商必须具备对网络各区域之间的访问进行过滤的能力，以降低网络安全事件的影响（例如病毒爆发期间实施端口过滤）。

远程访问和主机安全控制必须采用基于组的访问控制机制（例如员工组、分包商组），以限制对供应商网络中相关网络资源的访问。在主机层面，可根据用户组或个人身份实施访问控制。

17.46 网络设备识别

技术平台必须根据交互的 **IS** 风险等级以及其他缓解控制措施，对对端技术平台进行身份识别与身份验证。

1. 只有符合本要求并经供应商授权的供应商设备（即硬件，包括但不限于台式机和笔记本电脑）才能访问存储、处理或传输花旗信息的供应商网络。
2. 只有符合本要求并经花旗授权的供应商设备（即硬件，包括但不限于台式机、笔记本电脑和可移动数据存储介质）才能访问花旗网络。

17.47 安全需求分析与规范

供应商必须在应用程序、产品和服务的选择、开发及实施流程和程序中纳入信息安全相关流程。

17.48 在线交易

1. 如适用，供应商必须确保信息系统采用动态密码或数字证书来验证凭证。
2. 所有终端实体证书必须至少每 13 个月更换一次。
3. 存储、处理、管理或访问花旗信息，托管面向互联网的花旗品牌应用程序或连接到花旗网络资源的供应商应用程序必须：
 - a. 采用基于所访问的数据/功能类型的身份验证方法；
 - b. 评估多因素身份验证（MFA）合规性并在必要时实施相关建议；
 - c. 执行可疑活动监控（SAM）接入评估，并在必要时实施相关建议；
 - d. 在所有上述情况下，供应商应联系其主要业务联系人，了解花旗的现行要求。

17.49 变更控制程序

1. 供应商须确保，对防火墙、入侵检测系统（IDS）和入侵防御系统（IPS）的配置变更均通过供应商的变更管理流程传递。
2. 必须记录和监控通过临时 ID 授予的生产系统访问权限，以跟踪对环境所做的变更。
3. 对于所包含客户信息的花旗分类为机密或更高级别、“完整性”组件值为 IS 风险或者“可用性”为“高”的受控信息系统，供应商必须对根据第 17.32 节（审核记录）采集的日志进行检查。此类检查可采用适当的基于风险的抽样方法。
4. 复核必须验证，临时特权访问期间实施的变更是否符合预期。
5. 供应商必须记录所有变更，包括存储审查流程的证据。

17.50 信息泄露

供应商须制定记录在案的安全编码标准，以防止信息泄露，包括：

1. 详细的系统信息（例如：服务器类型和技术）。
2. 会泄露目录树结构以及底层数据库类型的堆栈跟踪信息和异常错误信息。

17.51 测试数据

供应商不得在软件应用程序开发或测试环境或实验室中使用或存储花旗定义的机密或更高级别信息，除非采用符合行业标准的工具和方法对该信息进行去识别化、伪装和/或模糊化处理，从而使此类数据不再属于敏感信息，否则供应商必须在开发或测试环境内落实实时生产控制措施。

17.52 系统验收

供应商必须具备符合相关行业标准的、有据可查的项目范围管理和系统验收流程。

17.53 报告信息安全漏洞

供应商必须设置相关流程，以确保[立即向花旗报告](#)导致花旗信息资产受到损害的应用程序和基础设施漏洞。

17.54 安全事件责任与处理流程

1. 安全事件响应团队（SIRT）定义的安全事件，是指无论安全事件发生的方式、地点，或造成安全损害的责任主体是谁，只要导致以下任一情况受到影响，即构成安全事件：
 - 花旗数据的机密性、完整性或可用性。
 - 花旗根据合同、法律或监管义务所承担的任何数据（包括个人信息）的机密性、完整性或可用性。
 - 存储、处理或传输任何花旗数据的花旗信息系统的完整性或可用性。
2. 就本文件而言，机密性受损是指数据向未经授权人员暴露，或花旗失去对数据的保管和控制权的情形。所有安全事件均须立即报告。
3. 如果供应商遭遇 SIRT 定义的安全事件，供应商必须配合花旗，根据花旗自身事件响应流程提供所需信息；以足够满足花旗法律、监管及内部治理要求的方式分析受影响数据；按照法律、法规或监管要求，或由花旗酌情决定并应花旗要求，在供应商承担费用的情况下发出任何和所有必要通知，且仅可在花旗有机会审查并修改拟议通知模板措辞后发出通知。供应商不得在任何此类通知中指明花旗名称，除非花旗明确书面要求其这样做。

17.55 数据泄露防护（DLP）

供应商必须实施数据泄露预防（DLP）控制措施，其中包括内容和端点监控，覆盖所有有权访问花旗机密或更高级别数据的员工。

供应商必须制定控制措施，以检测和防止花旗机密或更高级别的数据通过以下渠道从其网络上转移出去：

- a. 未加密的电子邮件
- b. 加密的电子邮件附件
- c. 打印花旗数据
- d. 将花旗数据传送到其网络之外的位置（例如通过 FTP）
- e. 尝试将花旗机密或更高级别数据复制到可移动介质，例如 USB 驱动器、可移动硬盘、CD/DVD 驱动器和其他具有数据存储功能的可移动设备。默认情况下应阻止这种特权。
- f. DLP 解决方案必须记录并提醒供应商所有构成将花旗机密或更高级别的数据从其网络移动、传输或复制到其他目的地的尝试（无论成功还是被阻止）的事件。默认情况下应阻止这种特权。
- g. 将花旗数据上传到外部网站，包括 SaaS/文件共享网站。默认情况下应阻止这种特权。

17.56 网络浏览

1. 供应商必须设立网络访问控制措施，以防止共享花旗机密或更高级别的信息，以及防止有权访问花旗数据的员工接触到恶意软件或受到攻击。
2. 对于有权访问花旗机密或更高级别数据的供应商：
 - a. 必须记录所有 URL 请求。
 - b. 必须阻止对可被用于未经授权共享花旗数据的网站（即网络邮件、聊天、社交媒体、在线存储、生成式人工智能等）的访问尝试。
 - c. 必须阻止访问可能使环境接触到恶意软件或受到攻击的网站。
 - d. 必须阻止对被视为与业务无关的网站的访问尝试。
 - e. 供应商必须订阅定期更新的 URL 分类服务；默认情况下必须阻止所有未分类的 URL，或默认情况下必须阻止所有 URL，并根据具体情况批准 URL。
 - f. 供应商所使用的网络浏览器必须得到全面支持，并已更新为最新版本且包含软件服务商提供的最新安全更新。

17.57 电子消息传递

不得使用即时消息、对等网络或其他互联网协作工具向供应商网络或包含花旗信息的网络以外传输花旗信息或将花旗信息存储在这些地方，除非根据第 17.9 节（加密控制措施使用政策）对所有花旗数据适当加密。

17.58 电子邮件

供应商必须采取电子邮件控制措施，以防止共享花旗信息以及接触到恶意软件或受到攻击。其中包括：

1. 对进入电子邮件网关的传入文件附件进行扫描，如果对系统构成风险则会被阻止。
2. 使用最新版本的电子邮件过滤（反垃圾邮件、反网络钓鱼）软件。
3. 任何花旗机密或更高级别的数据在发送到供应商的组织外部时都必须加密。
4. 供应商所使用的电子邮件客户端得到全面支持，并且是最新版本，包含软件服务商提供的最新安全更新。

17.59 可移动介质

1. 供应商必须保护花旗信息（不论其在哪种介质上维护）。该标准适用但不限于存储花旗信息的以下几类介质：卡、磁带、光碟（CD）、软盘或其他可移动存储设备、硬拷贝输出、磁盘、录音带、缩微胶卷、缩微平片、光盘或纸质文件。
2. 存储花旗信息系统的便携式存储介质/存储设备的默认访问权限必须设置为“禁止访问”。如果允许例外情况并授予读写权限，则必须在便携式存储介质上对数据进行加密。
3. 如果允许使用可移动存储介质，则必须经过管理层审批流程，包括说明使用可移动存储介质的业务理由。管理层必须对可移动存储介质进行清点。包含花旗机密或更高级别数据的可移动存储介质必须自动加密，无需用户进行任何操作。

17.60 介质处理

1. 在适合按花旗指示处置花旗机密或更高级别信息时（即，当这些信息对花旗不再必要或有用时，而且法律、法规和/或花旗政策所要求的任何额外保留期限已到期），供应商必须销毁相关信息，使其无法使用和恢复。
2. 必须使用一种认可的工具，以根据以下规则随机用特定的不同字符覆盖驱动器扇区来安全地擦除可挂载媒体：
 - a. 对于存储归类为“机密”或更高级别信息的介质，工具必须对该介质完成三次擦除操作。
 - b. 对介质进行消磁处理（如适用）。
3. 对介质进行物理销毁，使其无法读取（例如，粉碎、压碎驱动器）。
4. 包含机密或更高级别信息的纸质和其他非电子存储介质必须在最终处置前安全收集并存放在安全的“机密箱”中。机密箱必须始终上锁，并且只能由授权人员打开。
 - a. 复印机、打印机、传真机以及任何具有内存/存储功能且可能包含花旗机密或更高级别信息的设备，也必须进行数据清除。

17.61 信息安全管理与培训

1. 供应商必须维护适当的网络安全/信息安全意识和教育计划，包括但不限于：防范网络钓鱼及其他社会工程攻击、机密或更高级别信息的适当处理，以及安全事件报告和响应管理。
2. 供应商必须确保所有员工（包括承包商和临时员工）接受与其工作职能相关的组织政策和程序的相应意识教育和培训。
3. 供应商必须确保每年对培训和意识计划进行审查和更新，以应对网络安全环境中新出现的风险和威胁、采用行业当前最佳实践以及网络安全领域的新技术。
4. 必须至少包括以下主题：
 - b. 信息标记和处理
 - c. 安全传输（例如：安全电子邮件、安全 SharePoint 存储、禁止将花旗数据发送至个人电子邮箱）
 - d. 信息安全事件报告
 - e. 安全工作场所（例如：适当的互联网使用、禁止使用未经授权的软件以及禁止下载未经批准的软件）
 - f. 密码管理（例如：强密码、禁止共享密码）
 - g. 社会工程攻击（例如：网络钓鱼、鱼叉式网络钓鱼、语音钓鱼、短信钓鱼）
 - h. 远程办公（例如：安全连接/安全访问、个人设备安全）
5. 供应商员工必须在获得托管花旗数据的系统访问权限时或之前接受培训，并在分配通知中规定的截止日期前完成培训。
 - a. 在法律允许的情况下，应至少每年对所有人员进行一次 IS 培训。
6. 在当地法律允许的情况下，培训应包含用于记录培训有效性衡量结果的凭证或记录（例如：完成培训后的测验，并设定通过/未通过标准）。

17.62 网络风险管理计划

供应商还必须至少维护适当的网络风险管理计划，其中包括以下方面：

1. 维护定义明确、文档化的信息安全风险管理计划，和/或具有清晰定义的网络/信息风险管理组件的运营风险管理计划，从而定义供应商的网络风险偏好并确保其网络残余风险与偏好保持一致。
2. 维护稳健的安全风险管理管治计划，包括但不限于收集和/或执行安全审核和审查，以评估组织内的整体安全状态，并至少每年向其执行领导层报告一次以供审查，并确保未违背供应商的网络风险偏好。
3. 供应商在处理、存储和/或传输信用卡/借记卡交易、支付和/或信息时，务必遵守适用于供应商的任何 PCI 数据安全标准（PCI-DSS）。
4. 维护符合行业标准的危机管理计划和方案以及安全事件响应团队计划，以确保供应商有足够、充分的能力来检测、遏制、调查、应对任何未遂、疑似和/或实际的网络安全事件并从中恢复过来。

17.63 应用程序、API、代码、系统和基础设施安全

供应商进行托管、开发、合作开发、提供开发环境和/或提供软件应用程序时，应对所述软件和/或补丁进行代码审查以发现安全缺陷并防止未经授权访问、修改和/或插入恶意软件或其他形式的恶意代码以及漏洞测试，以确保应用程序（包括 API）以及其底层系统服务、操作系统和网络不存在已知漏洞和缺陷，避免导致安全事件、隐私泄露、欺诈、未经授权访问和/或机密信息泄露、应用程序处理/存储/传输信息的完整性丧失，和/或可能影响供应商向花旗提供的产品和服务质量的可用性丧失。

17.64 移动安全

如果供应商提供移动应用程序解决方案，则供应商必须遵守以下要求：

1. 移动应用程序必须仅支持 Google Android（不包括 Android Go）和/或 Apple iOS/iPadOS 平台的已正式发布（GA）、稳定和非 EOL²版本。如果移动解决方案可为更多平台提供支持，则花旗应能够配置所支持的操作系统/版本。
2. 移动解决方案不应支持未配备支持加密算法的常规指令集的移动平台/设备，其中包括但不限于本文档第 17.9 节（“加密要求”）中规定的加密算法。
3. 生产环境禁止使用预生产操作系统版本，包括但不限于测试版、抢先体验版和功能预览版/发布版。
4. 供应商必须能够提供集成的第三方组件列表，包括但不限于移动解决方案所捆绑/利用的自由和开源软件库。
5. 移动应用程序必须遵守相关要求和最佳实践，以使移动应用程序能够通过 Apple App Store 或 Google Play 等公共应用商店发布。所列出的公共应用程序商店应为分发/发布移动应用程序的首选和主要方式。
6. Android 移动应用程序必须利用 APK 签名方案 v2+。不得使用 APK 签名方案第 1 版（亦称 JAR 签名）。
7. 移动应用程序签名密钥类型和长度必须遵守本文档第 17.9 节“加密要求”的规定。
8. 每个应用程序签名密钥和相关 X.509v3 证书必须单独管理，并专用于单个应用程序 ID/捆绑包 ID。签名密钥不得在应用程序之间共享。
9. 如果移动应用程序需要在移动设备上保留数据，则必须仅在设备上保留应用/服务用途所需的最新数据，或者按照法律和/或监管要求的规定时长进行保留。
 - a. 用户数据的收集、处理和/或存储必须符合当地法律，包括但不限于隐私法规，例如《通用数据保护条例》（GDPR）和《2002/58/EC 电子隐私指令》或其区域等效法规。
 - b. 集成的第三方组件（例如库）不得收集、处理和/或存储用户数据。

² 此类产品版本得到积极支持并定期收到来自平台所有者或供应商的安全和维护更新。

10. 移动应用程序不得让任何应用程序数据具有全球可访问性。
 - a. 如果需要与其他应用程序共享数据，这些应用程序必须利用商业上合理的技术、方法和控制措施，使得此类数据共享有正当理由并记录在案，让相应操作系统只与数量极少的其他应用程序共享所需数量的数据。
11. 移动应用程序必须完全依赖相应移动操作系统提供的安全通信设施。例如，
 - a. **Android** 应用程序必须在其应用程序清单和/或网络配置文件中明确声明，禁止向任何网络域发送不安全网络流量。
 - b. **iOS/iPadOS** 应用程序必须使用应用程序传输安全（ATS），并且不得允许任何例外情况。
12. 加密材料应与基于硬件支持的安全密钥库绑定。
13. 移动应用程序必须以发布模式构建，并且不得包含以下内容：
 - a. 任何可能绕过安全控制措施的功能或方法；
 - b. 可能被用于逆向工程的调试信息，例如源代码文件名、变量名、符号名、注释等。
14. 移动应用程序必须配备有效的反挂接或反篡改机制，以防止在运行时注入可能改变或监控应用程序行为的恶意代码。
15. 移动应用程序必须实现全面的反调试或反逆向工程/混淆技术，以阻碍逆向工程攻击。
16. 移动应用程序包必须具备可以验证其内容真实性和完整性的能力（例如，使用密码校验和和/或数字签名）。
17. 如果移动应用程序需要用户身份验证，应在用户身份验证开始之前完成应用程序和/或设备完整性检查。
18. 如果访问/处理/存储花旗归类为“机密”或更高级别和/或其 **IS** 风险分类为“中”或更高级别的任何花旗拥有的信息，移动应用程序必须仅利用强生物识别模式（例如，达到或超过相应 [Android 兼容性定义文档](#) 中定义的 3 类/“强”类别）。
19. 移动应用程序必须实施对策来防止中间人（MitM）攻击。
20. 移动应用程序必须能够检测包括但不限于“已越狱”或“已获得超级管理员权限”移动设备在内的受损设备，并按照业务的风险评估和监管要求做出反应。
21. 移动应用程序必须实现强设备绑定，以防止软件令牌（例如所有权证明）被克隆。
22. 移动应用程序必须使用安全的键盘应用程序/解决方案（例如由移动操作系统内置/预先安装的应用程序）。
23. 推送通知不得包含任何敏感信息（例如归类为“机密”或更高级别的花旗信息）。但一次性密码（OTP）可通过推送通知方式发送。
24. 移动应用程序解决方案必须配备拒绝/忽略与使用具有已知/可利用漏洞的应用程序版本的移动客户端进行通信尝试的能力。
25. 移动应用程序必须遵守行业最佳实践，包括但不限于 [OWASP 10 大移动风险](#) 中公布的预防技术。

26. 利用人工智能和机器学习（AI/ML）技术的移动应用程序必须以合乎道德并且符合第 19 节“人工智能/机器学习（包括生成式 AI/智能体AI）”规定的方式进行。
27. 移动应用程序必须利用执行花旗利用的用途/功能所需的最低设备权限。
28. 移动应用程序不应在外部/移动存储介质（如 SD 卡）上存储任何非公开信息。

17.65 软件披露

供应商必须披露其向花旗提供的所有产品或服务中包含的软件组件，包括但不限于开源软件（统称“软件组件”）。未经事先向花旗披露，供应商不得通过更新、升级或其他任何方式，在任何将安装于花旗系统上的产品或服务版本中加入任何软件组件。此外，供应商还应确保其产品或服务不包含任何根据许可条款会使花旗或其关联公司承担未在协议中由花旗明确披露并接受任何义务的软件组件。供应商必须在发现其组织、产品或服务中存在恶意软件组件后的 30 日内通知花旗。具体而言，供应商应通过以 OWASP CycloneDX 文件格式或 ISO/IEC 5962:2021 软件包数据交换（“SPDX”）规范文件格式向花旗提供软件物料清单（“SBOM”），披露其在产品或服务的每次发布和版本上对软件组件的使用情况。此类披露必须包括包括软件组件的来源（例如：商业供应商、嵌入式数据库、公共二进制包管理器、从源代码构建、或任何嵌入式软件，以及经过筛选的软件组件提供商），并说明供应商或其软件供应链依赖方是否已获取该软件组件的副本（即“复刻”）并将其纳入其产品或服务中，无论是作为包依赖项，还是作为已集成至供应商源代码中的源代码（产品或服务即从此源代码编译而成）。

17.66 威胁建模

供应商必须实施威胁建模流程，该流程应全面涵盖以下所有内容：

1. 范围定义：供应商必须明确界定威胁模型的范围，重点关注处理、存储或传输花旗机密或更高级别信息的软件组件和数据流。
2. 威胁识别：供应商必须在设计生命周期的早期阶段，系统地识别与软件设计、架构和预期用途相关的潜在威胁和漏洞，并考虑各种攻击途径和威胁主体。
3. 风险分析：供应商必须分析已识别的威胁，评估其潜在影响和可能性，从而确定安全风险的优先级。
4. 控制措施集成：供应商必须在软件设计和开发过程中定义并集成适当的安全控制措施和风险缓解策略，以应对已确定的优先级安全风险。
5. 文件记录：供应商必须记录威胁模型，包括发现的威胁、相关风险以及实施的相应缓解措施。
6. 定期审查：供应商必须定期审查和更新威胁模型，尤其是在软件设计、功能或部署环境发生重大变化时。

17.67 人工智能

1. 供应商必须针对向花旗提供或与花旗集成的所有 AI/ML 系统和组件，实施并遵循稳健的安全软件开发生命周期（SSDLC）。这包括安全设计、开发、测试、部署和持续维护。

2. 供应商提供的 AI 系统必须展现出运行的完整性，并具备强大的抵御对抗性攻击的能力。这包括实施快速注入检测、输入清理和数据隔离机制。
3. 供应商提供的 AI 代理和组件必须能够与花旗的系统和其他工具进行安全交互。这需要强大的身份和访问管理、对工具执行参数的严格验证以及对高风险工具操作的隔离。对于敏感或高风险操作，必须采用人机协同（HITL）机制。
4. 供应商 AI 系统必须为所有重大事件生成全面、不可篡改且可审计的日志。这些日志必须受到保护，防止篡改，并根据花旗的政策进行汇总和保留。供应商 AI 系统必须具备持续监控和异常检测能力，以识别安全相关事件和可疑活动，并发出告警。
5. 供应商 AI 系统必须支持基于风险的人工监督，确保在必要时能够进行适当人工干预，并在系统设计中明确 AI 输出和操作行为的责任归属。这包括按照风险等级对 AI 输出进行分类，并提供人工覆盖功能。
6. 供应商提供的所有 AI 代理、组件和系统必须实施健全的身份与访问管理控制。所有 AI 交互必须能够追溯至明确可识别的身份（包括人工身份或非人工身份），所有访问均必须经过身份认证。AI 代理访问花旗资源时必须采用受管理身份，并遵循最小权限原则。
 - a. 供应商必须配置花旗对象身份网络（COIN）代理身份，确保所有 AI 代理均分配有这些身份，并与花旗身份和访问管理（IAM）系统建立身份联合，以支持应用花旗安全策略、集中化身份管理及可审计性。
 - b. 供应商必须使用花旗批准的集成机制，将第三方 AI 代理接入 COIN，包括通过安全网关（例如 SSG Gateway 或 Apigee）提供的 COIN API，并必须确保接入过程符合花旗适用的安全要求，以安全的方式完成。
 - c. 如果由内部托管，供应商必须生成符合 COIN 要求的令牌。如果采用外部托管并通过自有联合令牌进行入站身份验证，则需具备支持花旗令牌的交换令牌（例如从 MSFT 令牌交换为 COIN 令牌）。任何目前无法通过令牌交换机制支持的新令牌类型，均须由花旗 IAM 团队审核批准。
7. 如供应商使用或提供模型上下文协议（MCP）服务器或客户端，则必须实施 MCP RFC 7591 标准，并启用其中规定的所有可选功能。
8. 供应商 AI 系统必须保护系统提示及其内部工作机制，防止其被披露或遭到篡改。上下文管理必须实施严格的边界控制，以防止不同租户、用户或环境之间发生数据泄露。
9. 供应商必须制定书面程序，用于检测、响应和报告 AI 相关的安全事件，包括对抗性攻击、模型篡改、未经授权的 AI 操作或涉及 AI 系统的数据泄露。任何此类事件必须立即通知花旗。

18 安全工作场所准则

适用于以下供应商：访问/处理/管理/存储花旗信息；和/或托管面向互联网的花旗品牌应用程序；和/或连接到花旗网络资源；和/或需要独自进入花旗设施。

供应商必须保护花旗及其客户的有形和无形资产。花旗及客户资产只能按照经核准的方式（例如根据适用许可证、条款和条件）用于经核准的用途，并且仅限用于花旗及花旗供应商的业务用途。资产包括现金、证券、实体财产、服务、商业计划、花旗信息、供应商信息、经销商信息、知识产权（电脑程序、型号和其他物品）以及其他任何个人、专有和保密信息。滥用或未经授权擅自披露花旗资产违背了您对花旗负有的责任，并有可能构成对花旗的欺诈。同样，对花旗资产的疏忽、浪费或未经授权的使用也构成对花旗的违约行为。

项目	要求
花旗信息（电子和纸质文档）	在正常工作时间结束后以及供应商离开指定工作区域时，必须将花旗信息妥善锁存并妥善保管。
台式个人电脑（PC）和笔记本电脑	用于访问或查看任何花旗信息的台式电脑和笔记本电脑，必须在一段时间无操作后自动启用受密码保护的屏幕保护程序。供应商每次离开指定工作区域时，必须按 Ctrl + Alt + Del 并选择“锁定计算机”，以锁定电脑和/或笔记本电脑。若供应商使用笔记本电脑查看花旗信息，则必须确保在工作时间内使用防盗缆线或安全锁将笔记本电脑固定在基座设备上，并在正常工作时间结束后将其锁入安全地点妥善保管。
锁好保管	存放花旗信息的所有文件柜及抽屉，在正常工作时间结束后必须保持上锁状态。
开放式办公区	开放式办公区域不得用于部署存储花旗信息的文件服务器或小型数据中心，除非其专门为此用途设计，并已向花旗备案。
打印机、复印机和传真机托盘	所有与花旗相关的资料必须及时从打印机、复印机及传真机的输出托盘中取走，不得遗留。
处置	对于不再需要的花旗信息，必须按照适用的资料保留期限进行处置。纸质文件必须采用碎纸方式销毁，或投入安全且带锁的回收箱。磁性存储介质在按照规定完成安全擦除程序后，必须采用安全方式进行处置。

19 人工智能/机器学习（包括生成式 AI/代理式 AI）

适用于在其提供的产品或服务的任何部分中使用人工智能/机器学习（AI/ML）的供应商，包括花旗在《供应商要求》中定义的生成式 AI 和代理式 AI。

19.1 供应商不得使用，并确保任何分包商不得使用下述 AI/ML，除非双方已在合同项下适用的附表或工作说明书中就此类使用达成一致：

1. 用于、包含于或以其他方式集成于其根据合同直接或间接向花旗提供（或其任何部分）的任何产品或服务中，包括其中所含或嵌入的任何第三方产品或服务；或
2. 以任何方式用于供应商履行任何合同的过程中，无论此类 AI/ML 是否实际用于、包含于或以其他方式集成至交付给花旗的产品或服务中；或
3. 供应商以任何方式使用 AI/ML，且该使用可能导致花旗信息暴露于此类 AI/ML，包括但不限于供应商在其非商业性业务运营中使用的任何 AI/ML（例如业务记录管理、流程改进、研发、合规管理以及内部审计）。

19.2 供应商未能履行上述义务，将被视为对本协议条款的实质性违约。

19.3 如果监管机构提出要求，在监管机构针对产品/服务任何部分中 AI/ML 的使用情况开展监管检查或取证调查时，供应商必须协助花旗响应监管机构的要求，包括开展和/或协助开展必要的算法审计，以发现构成 AI/ML 模型的算法的实际运作情况。

19.4 还必须遵守以下原则：

合法性。 供应商 AI/ML 应遵守适用法律。

目的和相称性。 供应商不得将内容或花旗信息与供应商或任何第三方数据加以合并。未经花旗书面批准，供应商不得使用内容或花旗信息来训练 AI/ML。供应商 AI/ML 不得使用内容或花旗信息，但因提供服务所必需的情况除外。

20 客户投诉

20.1 投诉是一种口头或书面沟通，接收形式可以是口头（亲自或通过电话）或书面（通过邮件或电子邮件、聊天或社交媒体等电子通信），所表达的内容是客户、非客户、潜在客户、花旗客户、潜在顾客或顾客的授权代表（统称为“客户”）对花旗政策、由或通过花旗提供的产品或服务、花旗员工、花旗承包商、代表花旗行事的第三方服务提供商或上述任何组合的不满。

20.2 供应商必须遵守 Citi Customer Complaint Handling Policy，以及任何适用的花旗投诉相关标准和程序。供应商应在收到任何客户（或根据花旗投诉定义，包括非客户或潜在客户）或任何监管机构就供应商代表花旗提供的服务或与花旗相关的其他事项提出的任何书面或口头不满或疑虑（统称“投诉”）后二十四（24）小时内，以书面形式通知其主要花旗业务联系人（或指定人员）。除非花旗向供应商提供此类系统，否则供应商还应开发、实施和维护一套让花旗感到满意的系统（“跟踪系统”），以跟踪投诉并自行决定是否向花旗提供报告副本或访问系统的权限。跟踪系统将：

- a. 按类型、收到投诉日期以及向花旗提供投诉通知的日期对投诉进行分类，
- b. 跟踪投诉的处理过程直至结束/解决，以及

- c. 针对花旗可能合理要求的所有其他事项做好准备。跟踪系统的设计必须允许供应商确定其是否收到涉及特定事项的过多投诉，以便供应商（与花旗协商）可确定是否存在与供应商的业务或其提供服务有关的系统性问题并及时纠正问题。

21 个人交易和投资政策

花旗的 **Personal Trading and Investment Policy (PTIP)** 定义了允许和禁止的交易和投资活动、预先许可要求以及有关维护、披露和监督所涉人员的经纪或交易账户的要求。该政策规定了旨在促进遵守法律和法规的最低标准，以防止不当利用个人职位或与花旗的关系，包括个人对下列内容的了解：（1）有关花旗或第三方的重大非公开信息或内部信息（统称为“MNPI”）；或（2）有关客户的证券、衍生品和大宗商品头寸、交易和策略的信息。

需要定期访问 MNPI（作为其在花旗工作职责的一部分）并被指定为所涉人员和/或 **Citi Access** 人员的所有供应商人员都必须遵守 PTIP 中的要求。 供应商人员必须遵守 ICRM 关于个人账户披露、个人交易活动预先批准、个人交易限制和定期报表提交的要求。

22 计费和发票开具标准

为配合花旗改进服务及时性并加强控制措施的工作，所有供应商均应支持花旗首选的发票提交方式以及首选的发票付款选项，详见下文：

- 供应商将创建电子文件，以花旗向供应商传达的格式传送给花旗，并且/或者利用花旗供应商工具输入所需的发票/计费数据，以便随后以数字方式传送给花旗。
- 供应商将向花旗提供所有必要的银行信息和支持文件，以方便向供应商进行电子付款和/或利用花旗提供的虚拟卡支付方式（如可用）。

注：付款期限从花旗收到供应商提交的发票之日起计算。

为及时支付和履行合同承诺，花旗要求所有供应商包含以下发票数据，并在向花旗开具商品或服务账单时遵守相关指引：

1. 正确的花旗业务实体、“收单”地址以及相关花旗业务联系人姓名。
2. 发票编号、发票日期和采购订单编号。
3. 发票应寄至花旗办公地点或发送至花旗采购订单上详细注明的电子邮件地址。
4. 列入账单的商品或服务必须在发票中提供清晰、描述性的细节。

5. 仅包含特定发票的当前费用（不包含其他待结算发票的未付余额）。
6. 发票（包括证明文件）应使用英文。

23 强制休假政策

花旗的 **Mandatory Absence Policy** 要求从事敏感或高风险活动（尤其是涉及公司账簿和记录管理的活动）的人员定期离开其相关职责岗位。该强制性职责分离措施旨在通过创造发现潜在欺诈、盗窃或其他可能长期未被发现的不当行为的机会，加强内部控制。该政策符合美国联邦储备委员会就敏感岗位人员强制休假所设定的监管要求。

所有有权访问敏感数据且在花旗履行工作职责过程中被指定为“敏感人员”的供应商人员，均须遵守 **MA** 政策中的相关要求。敏感人员每年必须按照所有政策规定和限制，安排并完整履行强制休假期。在此期间，敏感人员不得执行、指示、授权或批准任何敏感活动，也不得对任何通信（包括与客户的互动）作实质性回复，但将咨询转交相关负责部门处理的情况除外。如强制休假期开始后需要中断，经理或花旗业务联系人必须在合规系统中取消该休假安排，以恢复系统访问权限。此后该人员须重新安排新的休假期。

附录 - 定义

网闸 (Air-Gap) 是指一种安全性措施，在实体上将电脑、系统或网络与其他电脑、系统或网络分开。使用网闸的数据备份架构可限制网络攻击的风险，并且可将数据恢复至攻击开始之前的某个时间点。

适用法律包括：(a) 州止赎法律和法规，以及 (b) 美国不同联邦机构发布的规则、指南和其他版本，包括美国货币监理署发布、用于落实 2003 年版《公平准确信用交易法案》第 114 条的文件（有时称为危险信号指引和法规）。

可用区为云服务提供商拥有一组逻辑数据中心的区域。可用区为云区内配有冗余电源、网络和电信的一个或多个独立的数据中心。

人工智能 (AI) 是指一种量化方法、系统或途径（“技术”），可通过计算机程序模拟人类智能，以优于传统的统计、数学、计量经济或金融方法的方式进行估算、预测、建议或决策。这包括如下所示的所有 AI 类别以及 AI 的各种形式和变体，例如：生成式 AI、代理式 AI、大语言模型、通用 AI (GPAI) 模型等。

AI 类别包括：

- **静态 AI**：指通过人工离线训练，或其参数被明确编程设定后，用于进行估算、预测、推荐或决策的 AI 技术。
- **动态 AI**：指不同于“静态 AI”的 AI 技术，该类技术能够在生产环境中定期自动重新训练其参数。
- **自动 AI**：指在“动态 AI”基础上，进一步具备自动改变其基本结构能力的 AI 技术（例如调整超参数、输入变量）。
- **认知 AI**：指能够自主进行决策并据此采取行动的 AI 技术，即使涉及的事项并非其最初接受专门训练的领域。

机器学习 (ML) 是 AI 的一个子集，指无需针对每个参数表示或计算步骤进行明确编程，而是通过数据自动学习并生成特征表示或推断结果的技术。例如，随机森林和基于神经网络的方法均属于机器学习技术。相比之下，不属于 ML 子集成员的 AI 技术，包括模糊逻辑以及用于自然语言处理的复杂依存句法分析技术等技术。

业务活动负责人 (BAO) 指负责执行和积极管理与供应商关系相关的某些活动的花旗员工。

业务介绍人是指花旗聘用的供应商，代表花旗行事以发现新的商机或管理现有客户关系。

商务礼品指花旗员工给予或收受的与花旗业务或外部方的业务有关的任何有值物品（商务款待除外），一般不包括价值为 25 美元或以下的物品。

花旗信息是指由花旗拥有，或花旗在存储、处理、传输或处置过程中负有保护义务的信息，包括数字格式和非数字格式的信息。

花旗信息分类包括：

机密信息是指与花旗业务和/或相关方有关，且不涉及个人信息、但需要采取高等级保护措施的信息。这些信息的机密性、完整性或可用性受到损害可能会对花旗的运营、财务状况

况、专有权或公司客户产生严重影响。

机密个人可识别信息是指涉及个人、有可能给针对该个人的身份盗窃、信用欺诈或其他金融欺诈等非法活动创造便利的信息。这些信息的机密性、完整性或可用性受到损害可能会对个人产生重要影响，包括但不限于经济损失或欺诈。

- 与其他个人数据结合后可构成机密个人身份信息（PII）的个人数据元素包括个人姓名或联系信息（地址、电话号码或电子邮件地址）与以下数据的组合：
 - 可能导致资金流转，或可能被用于身份盗窃、欺诈活动的交易相关数据，包括但不限于：
 - 信用卡/借记卡号码
 - 卡验证码（CVV）或个人识别码（PIN）
 - 信用报告数据（信用评分）
 - 完整出生日期
 - 员工绩效（评估/反馈）或薪酬信息
 - 视频监控录像，包括闭路电视（CCTV）录像及自动柜员机（ATM）录像记录
- 某些个人数据要素单独存在时即可构成机密 PII：
 - 美国社会保障号、政府签发的身份证号码（其用途和/或法律保护状态等同于美国社会保障号）、护照号、驾驶执照编号或个人税号。

内部信息是指并非作商业用途并需要适度保护的个人信息。这些信息的机密性、完整性或可用性受到损害可能会对团队或工作组产生**有限影响**。

- **个人可识别信息（PII）**是指任何具有以下特点的个人信息：
 - 识别或可用于识别个人或家庭（例如姓名、签名、地址、唯一国家身份标识符[如社会安全号、居民登记号]、出生日期、驾驶执照号）。
 - 与个人或家庭相关、描述个人或家庭，或能够（直接或间接）与个人或家庭合理关联。
 - 可用于验证个人身份或提供账户访问权限（例如：用户名、电子邮件地址、密码、PIN 码、身份证号码、安全问题答案）；或与个人相关且可能包含敏感信息（例如：个人医疗或健康信息、账号、账户余额）。
 - 个人信息还包括受保护的健康信息（根据美国《健康保险流通与责任法案》的定义）、敏感个人信息和信用信息（根据各项数据保护/隐私和银行保密法律的定义）。

公开信息是指可在花旗以外自由获取的信息，或供公共使用的信息，例如花旗的新闻稿或在有关花旗的新闻中出现的文章。

受限信息是指仅限特定人员或群体使用、对花旗或其关联公司而言最为敏感且需要最高程度保护的信息。这些信息的机密性、完整性或可用性受到损害可能会对花旗的运营、财务状况、专有权或公司客户产生**严重（全公司范围、多地区、多行业）影响**。

- **敏感 PII 信息**是指特定法律规定需要额外保护的个人信息，他人可能利用这些信息对个人实施非法歧视或以其他方式对个人造成不公平或伤害。这些信息的机密性、完整性或可用性受到损害可能会对个人产生重要影响（包括但不限于经济损失、欺诈或歧视性影响）。

- 具体涉及以下方面的数据：种族、宗教、宗教或哲学信仰、民族、政治派别或观点、工会成员身份、犯罪背景信息或犯罪记录、基因数据、生物识别数据，或有关个人性取向或性行为的数据。
 - 个人健康信息（PHI），包括有关个人病史或精神或身体状况的信息。

客户是指花旗的任何客户或顾客，包括个人（如自然人），以及企业、机构、组织和法律实体。

云区域是指云服务提供商集群数据中心所在的物理位置。

通信设备、系统和服务是指用于传输书面、语音或视频电子通信的任何硬件、软件或应用程序。电子通信渠道包括但不限于：计算机、笔记本电脑、平板电脑、移动设备或移动电话（包括“自带设备办公”[BYOD]）、黑莓手机、电话、传真服务、内联网和互联网接入、Wi-Fi 服务、电子邮件服务、即时通讯服务（例如 Microsoft Lync、Skype 和 Bloomberg Messages）、具有嵌入式通信功能的网站和应用程序、视频会议或协作平台（例如 Zoom 或 Microsoft Teams）以及社交媒体服务、交互式信息共享服务、第三方聊天室、电子公告板和博客。

内容是指花旗的机密信息，以及任何其他类型的数据、报告、统计资料或信息，包括：（a）由花旗或其关联公司，或由花旗或其关联公司的客户、顾客、服务提供商提供或代表其提供，并直接或间接向供应商提供或开放访问的信息；（b）通过服务创建或生成的信息；或（c）从上述任何信息中衍生出的信息。

合同是指由两方或多方签署的书面法律文件，其中包含要约、承诺、对价、各方义务以及目的合法性。合同示例包括产品和服务的主协议、工作说明书/工作单、修订和补充协议、附表、订单或花旗实体与供应商签署的任何其他书面文件。根据本标准，保密协议（NDA）也被视为合同。

拒绝访问（DOA）测试用于验证供应商针对花旗业务流程所提供的人员配置和支持能力，确保相关业务流程能够在规定的恢复时间目标（RTO）内恢复。

拒绝服务（DOS）测试用于验证供应商支持花旗业务的应用程序及其底层基础设施组件，确保其能够在规定的恢复时间目标（RTO）内恢复。

“寄存材料”指以下（i）-（vi）小节的统称，涉及（如适用）已授权花旗使用以便在花旗环境下运行的软件，或供应商为了向花旗提供托管服务而使用的材料：

- (i) 用于开发、运行、维护和支持与花旗签订的适用协议中规定的已授权软件或托管服务的软件源代码（以及此类软件或托管服务的所有后续版本）的精确复制版本，以及此类软件的所有文档（无论花旗是否可能已拥有此类源代码某些部分的副本）（“源代码寄存”）；
- (ii) 对于已授权软件或托管服务的开发、运行、维护和支持，供应商有权使用的任何第三方软件的“源代码”；
- (iii) 将寄存材料中包含的源代码转换为可执行格式所需的所有软件工具（如调试器、汇编器和编译器）的授权副本，该可执行格式对于软件或托管服务的运行、维护和支持必不可少；
- (iv) 如上述各项尚未提供，包含以下内容的任何文档：（A）寄存材料的一般描述和操作；（B）架构和基本程序功能；（C）数据流信息；（D）详细的内存映射和列表；（E）输入/输出端口映射；（F）此类其他细节，使得具有适用编程语言普通技能的程序员能够使用 and 修改寄存材料中包含的源代码；
- (v) 为使花旗或代表花旗的第三方能够使用、运行、修改和改进软件或托管服务，而合理要求的与软件或托管服务有关的所有其他技术信息；以及

(vi) 与软件或托管服务有关的所有第三方软件和技术列表，包括关于其在软件中使用的合理细节以及此类软件或技术提供商的联系信息。花旗承认并同意寄存材料未包含除 (ii) 小节所述以外第三方提供的任何源代码；以及

(vii) 关于托管服务：

- a. 云托管生产环境的缩小版副本，或与特定环境相关的云资源材料，以及复制花旗生产环境所需的其他相关信息，包括但不限于：基础设施即代码、环境改造脚本、云资源、云形成模板、配置文件、云租户、云订阅、机器镜像、Docker 镜像和基础设施即软件源代码；以及
- b. 存储于该软件中的花旗数据副本。

电子通信是指人员以电子手段发送、接收或使用的消息或信息，通过有线或无线信号传送皆可。电子通信包括但不限于短信、电子邮件、点对点或即时消息、博客文章、社交媒体帖子、通过 WhatsApp、微信、Line、Signal 或 Viber 等即时通讯应用程序发送的消息，以及附件、屏幕截图、录音或视频文件、实时语音或视频，以及通过电子通信设备、系统和服务创建、接收、下载、存储、传输、删除或使用的文件。

功能性 ID 是指一种通用 ID（如 ADMIN 或 ROOT），由个人或进程用于访问安全系统。身份与访问管理（IAM）运营团队的一项关键举措是确保花旗银行已建立明确且具体的安全控制措施，以防范与功能性 ID 使用相关的风险。

专有权关键流程/专有权关键应用程序（FCA）是指被花旗认定为对成功执行其专有权关键业务职能至关重要的流程/应用程序。

欺诈是指旨在欺骗他人并导致受害方遭受损失或实施欺诈者获得利益的故意行为、错误陈述或遗漏。

托管服务包括任何已安装的应用程序、供应商为提供托管服务而管理或使用的任何设施和环境，以及在托管服务环境中安装或使用的所有应用程序和其他软件、数据库、网站、服务器、硬件、网络、电信和其他设备及其他技术，并且在上述每种情况中均包括所有更新和支持服务，但不包括所有内容及花旗的系统。

身份验证数据（IVD）是指安全问题（SQ）或基于知识的身份验证（KBA）问题。安全问题通常由应用程序定义，由最终用户回答。例如：母亲的婚前姓氏、出生地点、最喜欢的冰淇淋等。这两类问题均须作为身份验证数据处理。

信息安全或“IS”是指计算机或计算机系统受到保护、不会遭受未经授权的访问或攻击的状态，该状态使（a）计算机或计算机系统持续可用和可操作；（b）计算机或计算机系统的完整性得到维护；（c）保存在计算机或计算机系统中、由计算机或计算机系统处理或通过计算机或计算机系统传输的信息的完整性和机密性得到维护。

IS 威胁指在计算机或计算机系统中执行的或者通过计算机或计算机系统执行的行为或活动（无论已知或可疑），此类行为或活动可能对该计算机或计算机系统或其他计算机或计算机系统的 IS 造成损害或不利影响。

IS 漏洞是指计算机或计算机系统中可被一个或多个 IS 威胁利用的任何漏洞。

非客户/非创收活动是指不涉及创收活动的业务关键活动，包括法律事务、监管监督、监管合规以及业务连续性相关活动。

保密协议（NDA）是指花旗与供应商之间签订的协议，该协议规定并约束信息的交换、使用及披露。

开源软件是指源代码或经编译的计算机程序，其中源代码向公众开放，可按照其原始设计用途进行使用或修改。

人员是指（无论明确表述或从上下文推断）供应商及其关联公司、董事、高管、员工、代理人、审计师、顾问、服务提供商和承包商（不包括花旗人员）。供应商人员还包括任何分包商的董事、高管、员工、代理人、审计师、顾问或其他代表。

记录清单是指对花旗记录进行详细登记的清单，包括记录类型、存储位置、日期等信息，用于支持业务部门按照信息生命周期要求对记录进行有效管理。

信息保留是指对记录和信息施加的一种限制，在发布保留令的机构解除限制之前，不得对其进行修改或处置。

恢复能力是指供应商产品和服务的交付量、数量或速度，以占正常交付量的百分比表示。

恢复持续时间是指供应商在恢复模式下能够维持运营的最长持续时间（以日历天数表示）。

恢复点目标是指业务中断后数据必须恢复到的过去某个时间点（以小时表示）。它是重大事件导致 IT 服务数据丢失的最大目标时间窗口。**RPO** 仅衡量重大事件影响 IT 服务时数据可能丢失的最大时间范围。它并非直接衡量可能丢失的数据量，例如，它并不意味着数据恢复点必然回退至前一工作日处理结束时的状态。

恢复时间目标指从服务中断之时到产品和服务恢复之时的持续时间。

“发布事件”指以下一项或多项：

- (i) 供应商（**A**）已资不抵债或承认债务到期时无力偿还；（**B**）自愿或非自愿地成为根据任何国内或外国破产法或资不抵债法提起的任何诉讼程序的主体，该诉讼程序未在七（7）个工作日内完全搁置，或在提起诉讼后四十五（45）天内未被驳回或撤销；（**C**）对债权人利益进行总体转让；或（**D**）拥有根据任何有司法管辖权的法院的命令委任的接收人、受托人、托管人或类似代理人，由其接管或出售其财产或业务的任何重要部分。

资源管理组织（RMO）负责花旗的全球端对端资源管理，包括战略采购、采购到付款业务、办公人员配置以及供应商管理框架。

RMO 采购经理是指资源管理组织（RMO）内负责合同业务条款、要求和定价谈判的人员，这些活动包括：招标书和其他供应商选择活动、合同条款和条件的管理以及财务评估认证要求。

对个人的**严重或灾难性不利影响**是指，该影响很可能对个人造成重大不利影响，包括经济损失、失业或就业困难、丧失人权、个人或公开羞辱，或者不适当的监禁。

分包商：分包商是指受第三方雇佣来执行花旗与该第三方签订合同的部分或全部服务或活动的第四方（个人或实体）。

指导：

Q1：是否需要报告所有的第三方分包商？

A1：仅需报告与所提供服务相关的分包商。分包商提供的服务或活动示例包括但不限于：

- *分包商提供技术或软件服务，直接或间接支持花旗与第三方签订合同约定的服务/活动；或
- *分包商提供的服务涉及访问花旗机密信息或更高级别的信息；或
- *分包商与任何现有/潜在花旗客户存在直接或间接互动；或
- *分包商在花旗任何场所内或场所外，在无人员陪同的情况下执行花旗文件的碎纸销毁或归档服务；或
- *为付款、收款、借贷等核心银行职能或服务提供支持的分包商。

供应商：就本《花旗对供应商的要求》文件而言，“供应商”专指已达成商业约定，直接向花旗实体提供产品或服务或者为花旗实体实现其业务目标提供支持的外部第三方。外部第三方指非花旗实体。供应商也可以是花旗实体的客户或顾客，或者支持与花旗客户和顾客进行互动；但仅基于其作为花旗的客户或顾客的约定不被视为本文件范围内的供应商关系。

临时信息：记录是指花旗因法律、监管或经批准的业务原因而必须保留的最终、最完整版本的信息。所有其他信息均归类为“临时信息”。