

CITI 供應商規定

擁有者：

Citi 採購與風險主管

發佈日期：

2015 年 1 月

修訂日期：

2026 年 9 月

版本：

9

目錄

1	總體概覽	4
2	平等就業機會	5
3	反賄賂及和反腐敗 (AB&C)	6
4	禮品及招待	6
5	供應商參與及供應商原則	7
6	禁止現代奴役	7
7	供應商人員	8
8	詐欺管理	9
9	媒體互動和公開露面	11
10	書面電子通訊	11
11	政治活動及獻金	12
12	反洗錢 (AML)	12
13	記錄管理	14
14	企業韌性/業務連續性	14
15	全球背景篩查標準	19
16	開支	21
17	資安 (IS)	22
18	安全工作場所指導方針	49
19	人工智慧/機器人學習 (包括生成式 AI/代理型 AI)	50
20	顧客投訴	51
21	個人交易及投資政策	52



22	計費及發票開立標準	52
23	強制離開職務政策	53
	附錄-定義.....	54

1 總體概覽

1.1. 一般規定

本《Citi 供應商規定》（以下簡稱「**規定**」）詳細說明供應商在與 Citi 進行業務往來過程中必須履行的一些義務。有些規定適用於所有供應商，而有些規定是否適用於特定供應商則視該供應商向 Citi 提供的產品和服務的類型而定（後者在下文第 1.2 節中有摘要說明，並在所列每項條款的開頭處註明）。重要術語具有本文中適用的含義（包括所附附錄中所述），除非本文並未表示該類含義，在這種情況下，則適用於合約中所述的含義，如以下所定義。

這些規定是屬於與 Citi 簽訂的供應商協議（包括但不限於交易文件，例如工作指令、授權排程）（每一項皆為「**合約**」）下的合約義務，而且是除了在任何協議下所特定的任何義務之外、任何在適用法律（該術語如下所定義）下的任何義務 Citi 向供應商發出的任何通知，通知供應商其在相同法律下的義務（每一項皆為「**通知**」），或 Citi 的業務或職能所實施的任何其他更具體的要求之外的規定。若上述任何規定與限制之間有任何衝突，則應採用較嚴格的義務與要求。供應商對於這些規定的任何問題，包括任何對其所做的變更、任何其所要求的豁免或任何在本文內或與適用法律間所認知的衝突，皆必須採取主動態度，諮詢其主要的 Citi 業務聯絡人（或指定人員）。

Citi 向供應商提交的任何 Citi 所需要的與供應商服務或人員相關資料的合理的要求，供應商都應立即提供，因為這些資料是 Citi 為了遵守適用法律的義務所需。供應商未能遵守這些義務將被視為重大違反本協議條款。

未能遵守這些規定或任何由與供應商有業務往來的 Citi 業務部門所要求的額外規定，將可能導致供應商與 Citi 的合約終止。此外，違反這些規定亦可能違反適用法律，且可能造成供應商對 Citi（或第三方）有民事損害賠償或刑事處罰之責任。供應商不得在未經 Citi 書面同意的情況下，藉由遵守其本身政策來替代遵守這些規定中任何條款的義務。

1.2. 適用於特定供應商的規定

下表列出適用於符合其中所指定適用標準的特定供應商的某些規定。未在以下所提及的章節則適用於所有供應商。

章節編號	章節標題	適用性
2	平等就業機會/平權行動	適用於 Citi 履行與美國聯邦政府合約所需的合約和採購訂單；如果不確定合約或採購訂單是否構成聯邦政府的外包合約或採購訂單，請在適當的情況下，在條款的開頭或結尾處加上「如適用」。
12	反洗錢	適用於執行與顧客相關的某些服務（即新顧客引導、顧客帳戶與交易篩查）或提供與上述活動相關的資料/指標的供應商；及/或擔任現金或金融工具（如遠端存款、快遞服務、運鈔車或收款箱服務）中間人的供應商。
13	記錄管理	適用於可存取 Citi 資訊，或處理、儲存 Citi 資訊的供應商。

章節編號	章節標題	適用性
14	業務連續性	適用於提供服務或託管 Citi 所使用的技術基礎設施/應用程式的供應商。Citi 業務活動負責人（BAO）負責傳達適用性和對供應商的 COB 規定。
15	全球背景篩查標準	適用於向 Citi 提供服務的供應商。
16	開支	適用於基於合約而有資格申請業務開支報銷的供應商。
17	資安（IS）	適用於可存取/處理/管理/儲存 Citi 資訊的供應商（包括分包商）；及/或負責託管 Citi 網際網路上的品牌應用程式的供應商；及/或可連結至 Citi 網絡資源的供應商；及/或要求無需陪同即可自行進入 Citi 設施的供應商。
18	安全工作場所指導方針	
19	人工智慧/機器人學習（包括生成式 AI/代理型 AI）	適用於使用人工智慧/機器學習（AI/ML）的供應商，如 Citi 在供應商所提供產品/服務的任何內容中所定義。
20	個人交易及投資政策	適用於基於在 Citi 工作的職責所需而必須定期存取 MNPI 的供應商。
23	強制離開職務政策	本政策適用於持有敏感職位（如詞彙表中定義）（「敏感工作人員」）的非員工，以及敏感員工的直屬經理和主管（「主管」），還有敏感非員工的業務聯絡人。

2 平等就業機會

2.1 平等就業機會

Citi 制定了旨在確保所有合資格的人士皆可獲得平等就業機會，不論其特徵為何，包括種族、膚色、宗教、性別、性取向、性別認同、民族起源、公民身份、移民身份、年齡、婚姻狀態、基因資訊、殘障、受保護的退伍軍人身份或任何其他受法律保護的特徵。

供應商應遵守並應確保其人員遵守所有適用之反歧視法律及法規的要求，包括但不限於 Citi 以書面通知供應商必須遵守的任何該等法律或法規。

供應商應根據 Citi 的《U.S. Equal Employment Opportunity Policy 聲明》審查並採取適當行動，此項聲明可在 www.citigroup.com/global/eeo-aa-policy 上找到。

2.2 政府合約

履行 Citi 與聯邦政府合約所需的合約和採購訂單必須逐字包含以下條款，並以粗體字體顯示如下。（如果不確定是否屬於聯邦政府的分包/採購訂單，建議在該部分的開頭處加上「如適用」）。

【如適用】 供應商將遵守所有適用的聯邦反歧視法律，並證明他們執行的計劃皆不會違反任何適用的聯邦反歧視法律

2.3 政府合約附錄

履行 Citi 與聯邦政府合約所需的合約和採購訂單必須在分包合約或採購訂單的附錄中包含以下聲明。（如果不確定是否是聯邦政府的分包/採購訂單，請在以下聲明結尾處加上「如適用」。）

身為聯邦政府的承包商，Citigroup 特此代表受保護的退伍軍人和殘障人士向以下署名的承包商或供應商提供關於我們平等就業機會義務的書面聲明。Citigroup 完全遵守《復健法案》第 503 條和《越南時代退伍軍人調整援助法》，以及根據 41 C.F.R. § 60-741 和 41 C.F.R. § 60-300 各別適用的法規。我們的《Equal Employment Opportunity Policy 聲明》詳列於 www.citigroup.com/global/eeo-aa-policy。如對我們 EEO 政策 Policy 聲明有任何疑問，請聯絡我們政策聲明中所提供的聯絡人。

【如適用】，我們要求您根據我們的政策聲明和法規採取適當的行動。

3 反賄賂及和反腐敗（AB&C）

Citi 已設有與遵守適用的 AB&C 法律相關的政策、程序和內部控管機制，並且嚴格禁止任何形式的賄賂或疏通費。供應商（包括業務介紹人）、其人員，或任何直接或間接代表 Citi 行事的人士都應秉持最高道德標準，並遵守美國《海外反腐敗法》（FCPA）、《英國反賄賂法》（UKBA），及 Citi 營運所在國家的所有其他適用的當地 AB&C 法律。

代表 Citi 行事的供應商或任何其人員，或與供應商與 Citi 之任何協議或關係有關的供應商及其人員，皆 (i) 不得向任何人支付、授予、授權或提供任何付款、利益、優勢或任何其他有價之物；或不得 (ii) 收取或接受任何人的任何付款、利益、優勢或任何其他有價之物；以上 (i)-(ii) 每個情況皆違反 FCPA、UKBA 或任何其他 AB&C 法律。供應商及其人員必須遵守這些規定（包括本節）以代表 Citi 執行其活動及交易，或任何與此供應商協議或與 Citi 關係有關之活動及交易。供應商及其人員還必須具備一份 AB&C 合規計劃，以及旨在確保供應商遵守所有 AB&C 法律並且予以應用的政策及程序。

如需查看 Citi 的 AB&C 計劃概述，請造訪 [Citigroup's Investor Relations](#)（請在「Citi 政策」項下，選擇「AB&C 計劃」）。

4 禮品及招待

供應商或其人員不得向 Citi 員工提供禮品或任何有價之物（包括招待），因這樣會產生實際或明顯的利益衝突，或是對等交換，或有損員工的誠信或判斷力或影響員工所作出的決定，或造成員工作出有違職責之事或違反相關法律。在不影響前述規定之前提下，員

工必須遵守禮品及娛樂（G&E）標準中的「禁止禮品及娛樂部分」中的規定。供應商及其人員每年不得向任何 Citi 員工提供總額超過 300 美元之非現金商務禮品。

供應商向 Citi 員工提供商務招待（例如邀請吃飯、體育活動、文化活動或其他類似活動）時，供應商也應參加該活動。此項招待必須恰當、合乎習俗及合理、不奢華或過於頻繁。此外，如果供應商未出席該活動，則這項娛樂將被視為商務禮品，並須遵守適用的 Citi 禮品及娛樂標準舉報門檻。供應商不得代表 Citi（或假借 Citi 名義）以供應商自費或由 Citi 員工付費的方式直接或間接向任何人提供任何有價之物，或誘導他人這樣做，因為這樣將會被視為或合理被視為貪腐、不當或違反適用法律。

5 供應商參與及供應商原則

<https://www.citigroup.com/citi/suppliers/> Citi 透過多項舉措鼓勵供應商參與，並向我們所服務社區的潛在供應商提高對 Citi 採購計劃的認識。此外，這些參與的計劃也尋求找出有潛力的供應商，特別是推動創新解決方法以解決新出現的業務問題的供應商。如欲瞭解 Citi 對供應商期望的更多資訊，請瀏覽 [Doing Business with Citi](#) 網站中的：

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

6 禁止現代奴役

Citi 致力於維護旨在識別和尋求防範在其組織內或其供應鏈中可能會發生的現代奴隸及人口販賣的風險的有效辦法。Citi 的供應商應遵守以下載明的各項規定，並制定整個企業適用的有效政策、程序及/或實踐做法，以識別並尋求避免在其本身的營運和供應鏈中的現代奴隸和人口販賣的風險。供應商必須應 Citi 的要求填寫 Citi 的「企業責任問卷」，包括必要時的任何其他資訊以便 Citi 能夠評估曝險情況和任何潛在的風險消除措施，尤其是在高風險行業和地理區域內營運的供應商。供應商的分包商應遵循相同的流程。

6.1 不得使用童工

供應商不得僱用兒童勞工。「兒童」一詞是指在適用法律下任何低於最低就業年齡的人，或如果沒有此類法律時，則是指 15 歲以下或低於完成義務教育的年齡的任何人，且以年齡較大者為準。如果未禁止使用童工且受僱勞工不滿 18 歲，則應特別注意他們所要履行的職務和工作條件，以確保他們不會因此工作或工作條件而直接或間接造成身體、精神或其他方面的傷害。

6.2 自由擇業

供應商應確保勞工不受到強迫、精神上或身體上的脅迫、被作為抵押、成為契約奴隸或遭受非自願監獄勞動或被販賣成奴隸，或受到任何形式的強制勞動，包括強迫加班。所有工作的進行皆應出於自願。供應商在本規定中的義務包括但不限於確保以下各項：

1. **合約、工資及工作時間：**勞工之受僱或聘用條款應以書面文件載明，且內容應易於瞭解並明確規定其權利和義務。這份書面文件應包括但不限於關於工資、

加班費、支薪期間、工作時數及休息時間與假日放假權利等的透明條款。此類書面條款應於勞工正式開始工作前提供給勞工且由僱主遵守，並應符合業界標準與工作所在地的適用法律及集體協議的最低要求。

2. **自由終止工作的權利：**勞工有權根據適用法律和集體協議，在經過合理的通知期限後可自由終止其工作而不得遭到不當處罰。
3. **不人道對待：**勞工、其家屬以及與其關係密切之人士不應受到嚴厲或不人道待遇，包括但不限於體罰；身體、心理或性方面的暴力或脅迫、辱罵、騷擾或恐嚇。移工、其家屬以及與其關係密切之人士不得因其國籍而在工作條款或條件上受到歧視。
4. **工資、福利及工作時數：**薪酬應符合所有適用的工資法律，包括與最低工資、加班時間和法定福利有關的法律。員工支薪應準時且全額支付，並附帶清楚的薪資明細。員工不得因紀律處分而從其薪資或福利中進行懲罰性扣除或扣留。每週工時不得超過當地法律規定之最長工時，且加班必須為自願性、在法律上限內，同時，拒絕加班不得遭到處罰。
5. **不得沒收身份證件：**勞工之身份或旅行證件、護照或其他正式文件或任何其他有價物品，不應作為僱用條件而被沒收或扣留，且財產的扣留不得直接或間接用於限制勞工之自由，或造成工作場所奴隸制。
6. **無招聘費用或負債擔保：**與招聘勞工有關之費用或支出（包括但不限於：工作簽證相關費用、旅行支出和文件處理費用），不得直接或間接向勞工收取。同樣，不得要求工人支付意圖或效果上造成工作場所奴役的款項，包括保障金，或要求透過工作償還債務。如果確定已向勞工收取與聘僱過程有關的費用或收費，或在聘僱過程中產生費用或收費，供應商應採取合理方法讓這些費用報銷。若必須透過第三方（如人力仲介機構）招聘勞工時，則僅能僱用信譽良好之第三方機構進行。直接招聘員工時，只能與信譽良好的招聘機構合作。禁止勞工支付招聘費用適用於所有招聘公司、代理商及子代理商。供應商應設有控管機制以確保恪遵此項規定。**行動自由：**勞工應可自由行動而不受任何不合理的限制，且不應在身體上受限於工作場所或其他僱主控制地點（例如，住宿區）的限制。除非因執行工作的地點或性質需要外，不得要求勞工必須住在僱主控制的場所。
7. **不得對於申訴進行報復：**勞工應有向僱主申訴不滿僱主對待之自由，且不得因提出該申訴而遭到不利影響、報復或迫害。

7 供應商人員

7.1 供應商人員培訓、工作指派、重新指派與管理。

供應商將使用足夠人數且具備適當培訓、教育、經驗和技能的人員，以符合任何合約的最有效方式執行服務，並可應要求證實此類人員的資格。在人員被指派到某專案後，若未經 Citi 的事先書面同意，供應商不得重新指派或使用該人員從事其他會減少該人員執行此專案工作的時間的事務，並且，在指派人員從事專案工作時，通常會將因需要重新訓練人員而造成中斷的情況降至最低。供應商將確保其人員不得自視為 Citi 的員工或代理人，也不得基於任何目的而尋求被視為 Citi 員工，包括聲稱有權獲得 Citi 提供的附加福利或殘疾收入、社會保險稅或福利、聯邦失業稅、州失業保險福利或聯邦所得稅預扣稅。供應商將全權負責有關其人員與所有與僱主相關的責任，包括但不限於維持所有必需的保險承保、進行所有適用的報稅申報，並以獨立承包商的供應商身份支付所有必需的稅款和預付稅款。

7.2 替換供應商的人員

如果 Citi 通知供應商，Citi 因任何其他非歧視原因無法接受某位被指派至某專案的人員時，供應商將另行指派人員以替換該員。供應商進一步同意，當供應商指派給某專案的人員無法或不願意以及時且專業的方式提供服務時，供應商將立即撤換該員並且提供替換人員，並禁止該員再為 Citi 提供服務（或與服務的交付或監督有關的任何責任）。

7.3 供應商的人事政策

供應商表示、保證和承諾，能維護和有效管理全面政策和程序，使被指派至 Citi 提供現場服務的自然人人員符合相關資格，且這些政策和流程包括工作授權驗證、工作經歷和犯罪記錄的背景調查（如本文內的進一步說明），以及職前藥物測試等，所有這些都要達到在任何適用法律及任何適用的勞資談判協議所允許的範圍內。在不受前述一般性的限制之下，供應商進一步表示、保證和承諾具備確保供應商完全遵守所有與移民相關的適用法律的控管機制和流程，包括確認指派至 Citi 的所有供應商人員都有權在整個任務期間工作，完全遵守所有與移民相關的適用法律。在要求之下，供應商將立即向 Citi 提供任何或所有指派至 Citi 的供應商人員的工作授權，及他們遵守與移民相關的適用法律的書面證據，並將不符合適用法律的工作授權的人員替換成有適當資格的人員，包括提供所有必要的培訓和入職指導，以確保可提供及時與有效的服務，且在任何情況下均不會對 Citi 造成額外費用。

7.4 供應商所有權

為了遵守 Citi 在經營業務所在司法管轄區的適用法律和法規，在 Citi 要求下，供應商有義務提供所有權人為自然人和/或法人的資料，包括透過影響力或其他方式直接或間接擁有或控制業務、產品或服務的供應商直接所有人到最終受益所有人。

8 詐欺管理

與 Citi 識別詐欺風險和消除詐欺風險相關的事宜（「詐欺管理」）。

8.1 所有供應商皆應：

1. 在法律允許的最大範圍內，配合 Citi 對可疑或涉嫌盜竊、詐欺或其他潛在犯罪活動或不當行為的任何調查，以及對詐欺或犯罪行為的任何起訴；

2. 確保使用 [Ethics Hotline](#) 及時向 Citi 通報並轉介任何潛在的詐欺事件。其中包括但不限於涉及 Citi、Citi 員工、Citi 供應商或代理人或非 Citi 員工（例如，臨時工和約聘人員）所為之未遂、嫌疑、涉嫌或實際盜竊、詐欺（例如，提供關於供應商、計費辦法、消失之資金或證券等明知為虛假、不正確或不實的資料）、犯罪活動或不法行為；
3. 允許 Citi 及其代表進行監控和監督，並支援 Citi 和執法部門所帶領對於涉及此供應商的潛在詐欺活動之調查。
4. 供應商一知道任何利益衝突便及時舉報（包括供應商/供應商人員和/或 Citi 員工之間的利益衝突）；以及
5. 在 Citi 的供應商支付系統中設定或更新供應商的銀行帳戶期間，支援 Citi 的詐欺防範流程。

8.2 除此之外，提供本質上更容易受到詐欺風險的服務的供應商必須：

1. 記錄並遵循詐欺風險管理計劃；此計劃可辨識與供應商提供給 Citi 的服務有關的重大詐欺風險，並指出可消除這些風險而實施的控管和程序；
2. 完成詐欺意識培訓（在聘用後的 90 個日曆天內，此後每年一次），並就與向 Citi 提供的特定服務相關的詐欺風險之特定要素對員工進行培訓；以及
3. 監控企圖詐欺的情形並維持有效控管，以消除他們提供給 Citi 的服務之詐欺風險，持續記錄控管程序和測試控管的有效性，並向業務活動負責人（BAO）報告任何缺失。
4. 提供任何規定的資訊，以執行盡職調查/持續監控/評估業務活動負責人（BAO）曝露於詐欺的風險。
5. 盡職調查包括第三方詐欺影響評估範本（簡稱「TP-FIAT」），此範本目的是對供應商消除詐欺風險的能力執行控管評估。本操作程序說明業務活動負責人（BAO）或第三方主管（TPO）和詐欺風險管理主管（FRMO）將執行的一組步驟，以識別和管理詐欺風險。

8.3 本身具有更高詐欺風險的供應商包括但不限於以下這類供應商：

1. 有權存取被分類為機密或更高層級的資料（如果並非由 Citi 直接控制或監督），可被用來進行詐欺，例如存取內部帳戶、金融交易、現金交易。
2. 可連線到 Citi 網路/系統；以及
3. 提供、支援或有權存取可能造成或促成詐欺的特定服務和能力，包括：
 - a) 新客戶的身份確認、開戶或申請處理。
 - b) Citi 或客戶付款/資金轉帳活動，及/或驗證存取這些服務的 Citi 客戶；
 - c) 對 Citi 資訊或 Citi 客戶端（如人口統計）資訊作出變更、檢查或履行變更；
 - d) 提供交易工具（如扣帳卡/信用卡、電子錢包、支票簿等），或為交易工具提供服務或授權；

- e) 向 Citi 提供或支援與詐欺事件預防、偵測或應變相關的營運詐欺管理活動。
- f) 提供實際取得現金、金融工具及資產/實物的能力；
- g) 可在無需陪同的情況下或下班時間進入 Citi 設施；
- h) 財務報表：帳戶活動，例如過帳至總帳/明細分類帳；
- i) 賺取及消費激勵活動的獎勵。

9 媒體互動和公開露面

Citi 企業服務與公共事務部是唯一被授權代表 Citi 發佈新聞稿或公開聲明的部門。供應商不得發佈任何直接或間接提及 Citi、供應商與 Citi 之間任何合約或安排，或 Citi 向供應商採購之任何產品和服務的新聞稿。未事先獲得 Citi 業務主要聯絡人之書面同意前，供應商不得同意或與客戶、Citi 員工、其他 Citi 供應商、供應商之其他顧客或任何其他第三方一起參加有關 Citi 之任何公關活動。

未事先獲得 Citi 業務主要聯絡人及資深國家公共事務主管之書面同意時，供應商不得以書面或電子形式公佈或貼文提及 Citi、Citi 之營運、Citi 客戶、產品或服務，包括書籍、文章、播客、網路廣播、部落格、網站貼文、照片、影片、社群媒體或其他媒體，亦不得於演講、接受採訪或公開露面時提及。

無論是否與向 Citi 提供服務或產品有關，供應商若未獲得 Citi 之書面同意，則於任何時候皆不得使用 Citi 之專有標記、商標、服務標章、商業名稱、標誌、符號或品牌名稱。供應商不得為 Citi 之外之利益或工作而使用 Citi 之名稱、標誌或商標，設施或夥伴關係（包括於信箋抬頭、個人網站、部落格或其他社群網站上使用）。此外，供應商亦不得出於慈善或公益之目的，使用 Citi 之名稱、設施或夥伴關係。

10 書面電子通訊

在與 Citi 人員互動，或為 Citi 或代表 Citi 履行其義務時，供應商僅可使用 Citi 核准的書面電子通訊設備、系統和服務。新的、擴充的或修正的 Citi eComm 頻道，無論是作為獨立工具還是整合到 Citi 提供的或第三方的更廣大平台中，都必須根據適用的 Citi 規定得到核准，供應商的 BAO 已透過書面通知供應商該規定。與 Citi 人員在溝通 Citi 業務時禁止使用非 Citi 核准的訊息傳輸平台，例如 WhatsApp、WeChat、LINE、Slack、Signal、Telegram、iMessage、SMS、Viber，及任何其他互動式電子平台。

此外，關於透過 Citi 提供的通訊設備、系統及服務所建立、發現、使用、存取、下載、儲存、傳輸、接收或刪除的書面電子通訊，供應商不應預期享有隱私權。Citi 得監控電子通訊設備、系統及服務，以及電子通訊。此類電子通訊由 Citi 擁有，並且可根據相關的記錄保留規定予以保留（必須遵循當地法律及法規）。

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

11 政治活動及獻金

與諸如以下相關的多種法律：外國影響力；競選經費；禮品及招待；立法遊說、草根遊說、親善遊說、監管遊說；採購、付費服務；以及證券、監管與 Citi 及其供應商有關的政治活動及披露事項。供應商不得從事任何不符合 Citi 相關政策或標準、法律或法規的政治活動。

政治活動包括但不限於：

1. 利用公司資金或資源（如設施、設備、軟體或人員）為公司或個人向政治團體捐款、募集政治捐款、或在公司工作時間為競選公職的候選人、政黨委員會或政治委員會義務提供個人服務；
2. 無論是直接或透過第三方，遊說公職人員或主動接觸公職人員，包括企圖影響政府官員、立法，以及視不同的司法管轄區而定，還可能包括企圖影響機構之立法或政府合約之授予；或
3. 尋求、接受或擔任任何與政府相關之政治職務，包括任何政府部門、委員會或其他類似組織。

未經 Citi 政府事務全球營運控管（ggacontrol@citi.com）的事先書面授權，任何供應商皆不得代表 Citi（或假借 Citi 名義）或其客戶參與或從事政治活動。雖然 Citi 可能會對供應商所提供的簽有合約且許可的政治活動服務（如遊說）支付費用及/或償付其自付墊款，但 Citi 絕對不會對供應商或任何其員工的任何種類的個人或企業的政治獻金提供償付。

12 反洗錢（AML）

適用於執行某些與顧客相關的服務（即新顧客引導、顧客帳戶與交易篩查）或提供與上述活動相關的資料指標的供應商；及/或供應商擔任與金融交易或金融工具相關（如遠端存款、快遞服務、運鈔車或收款箱服務、電子轉帳、數位資產）的中間人。

12.1 反洗錢（AML）義務：

1. 遵守 Citi 流程和適用法律：

- 持續維持並遵守旨在處理適用法律規定的流程和程序，包括 (i) 《格雷姆-里奇-比利雷法案》（Gramm-Leach-Bliley Act）以及根據該法案所頒佈的法規；(ii) 《美國愛國者法案》（USA PATRIOT Act）以及根據該法案所頒佈的法規；(iii) 任何有關洗錢的法律或法規；以及 (iv) 任何與經濟制裁相關的法律或法規。此類政策與程序將處理反洗錢職務與責任，包括對任

何觀察到的與金融活動、交易、現金收受等相關的異常或可能異常的活動需要立即舉報的規定。

2. 員工年度培訓與計劃要素：

- 確保這些向 Citi 提供服務的公司人員每年接受反洗錢職務及責任培訓，包括對任何觀察到與金融活動、交易、現金收受相關的異常或可能異常的活動要立即舉報的規定。培訓應包括但不限於以下項目：
- a. 舉報和向上呈報可疑活動。
- b. 「瞭解您的顧客」（KYC）計劃，包括顧客識別計劃（CIP）、制裁和名稱篩查、顧客盡職調查（CDD）、強化的盡職調查（EDD），以及識別並驗證最終受益人（UBO）。
- c. 所有相關金融工具及活動的交易監控。
- d. 定期報告/指標，包括法律和監管變更及重大 AML 計劃變更的報告
- e. AML 計劃有效性的測試和控管，包括現場訪查。

3. 遵守合約條款：

- 遵守合約中關於供應商必須實施的任何計劃的規定。

4. 立即舉報可疑的違規行為：

- 凡是可疑的違法行為都必須立即以書面向 Citi 舉報，包括觀察到 Citi 或其顧客的現金收受、金融活動、交易等的異常或可能異常的任何活動。

5. 防範逃稅與舉報：

- 遵守營業所在國家所有適用的稅法及法規。
- 在任何情況下，供應商皆不得故意涉及非法逃稅或代表他人進行逃稅，包括協助規避到期或應繳稅金，或向稅務當局隱藏資訊。
- 因此，供應商應對逃稅採行合理的防範步驟，並且立即以書面方式向 Citi 舉報任何與 Citi 有關的違法或可疑違法行為。

12.2 供應商內部政策和流程：

供應商應具備適當的內部政策和程序，以遵守所有現行或以後生效的反洗錢法律和法規。

13 記錄管理

適用於可存取/處理/儲存 Citi 資訊的供應商。

Citi 要求所有保管 Citi 資訊之供應商與其業務活動負責人（「BAO」）或 Citi 業務主要聯絡人合作，以 (i) 識別資訊並將資訊分類為「記錄」（Records）或「暫時資訊」（Transitory），以達成 Citi 記錄管理之目的、(ii) 按照 Citi 的主記錄目錄（「MRC」）對記錄進行分類、(iii) 根據 Citi 保存規定保存資訊，以及 (iv) 如果沒有「保留資訊」要求，則於資訊生命週期結束時妥善處置資訊。

BAO 或 Citi 業務主要聯絡人必須與供應商共同確保供應商已根據 Citi 在 MRC 中的記錄代碼辨識出記錄並進行分類，且庫存至少每年更新一次。供應商有義務遵守 BAO 所傳達之記錄管理規定。符合其處置資格標準的記錄必須盡快以適當的方式處置，除非有「保留資訊」的規定，否則最遲不得超過六個月。除非有「保留資訊」的規定，否則「暫時資訊」必須在最後一次使用後的兩年內銷毀。包括個人資訊的「暫時資訊」，一旦達成收集目的後即須刪除，除非有「保留資訊」的規定。接獲告知有「保留資訊」要求時，供應商必須暫停銷毀或修改 Citi 資訊。如有任何不確定之處，供應商應向 Citi 業務主要聯絡人或 BAO 查詢。

對於列於國家保留時間表中的保留規則每季進行審查及視需要進行更新，以符合 DRIM 對於監管和內部作出的變更。如果有影響到供應商的變更，BAO 將通知供應商。供應商應評估影響力，並實施個別系統、流程和庫存的變更。自 BAO 通知之日起 90 天內，擁有並管理的記錄類型。

代表 Citi 維護文件的供應商要負責在 BAO 要求的規定時間內保存（「持有」）、收集和提出被認為與法律或其他程序相關的所有資訊。供應商應因應要求，根據適用的合約條款退回 Citi 資訊。未經其 Citi 業務主要聯絡人或 BAO 之核准，供應商不得處置任何 Citi 資訊，無論其分類（例如機密、非機密）；核准必須包括確認沒有有效的「資訊保留」適用屆臨銷毀之資訊。除非另有明確約定，否則記錄管理與保存規定及所有其他資訊處理規定在合約終止或到期後仍繼續有效。

供應商應保有列出負責監督在其保管下的 Citi 資訊之所有供應商人員的文件記錄清單，並與 Citi 業務主要聯絡人或記錄管理主管定期召開會議，審查並更新聯絡人姓名、程序細節、職務和責任，以及供應商的 Citi 記錄資料庫。

14 企業韌性/業務連續性

適用於提供服務或託管 Citi 所使用的技術基礎設施/應用程式的供應商。Citi 業務活動負責人（BAO）負責傳達適用性和對供應商的 COB 規定。

14.1 復原資源

供應商的災難復原計劃必須提供可於供應商主要地點發生癱瘓時，向 Citi 提供所有產品及服務的備用資源。復原資源所處位置，應於地理位置上遠離主要地點，藉由完全不同的地理區，將可降低或消除同一災難事件可能影響主要及復原地點之威脅。

1. 復原資源不限於資訊系統，亦包括向 Citi 持續交付產品及服務所需之所有資源，可能包括人員、建築物、業務設備、資料中心、資料及語音網路及運輸服務。
2. 應用程式的供應商可執行雙機（Hot/Hot）熱備型架構，以確保高可用性（HA）配置。這個架構要求至少有兩個完全相同配置的系統在運行中並可供客戶/使用者使用。此模式最重要的特徵是備用環境與主要（正式上線）資料中心同時運作。

14.2 復原服務層級

供應商的業務連續性必須符合既定的服務級別，以向 Citi 提供有效服務。供應商的災難復原計劃至少應為以下各項設立具體數值：

1. 復原時間目標
2. 復原點目標
3. 復原資源/技術能力
4. 復原持續時間

14.3 災難復原計劃

供應商將具備一份可持續業務運作的災難復原計劃（並應 Citi 要求，提供其計劃的目前測試及定期測試的證據），以確保即使供應商在任何特定地點或透過特定人員努力提供產品/服務或履行其在本協議下的其他義務時遭遇任何中斷，仍然能夠迅速從替代地點或透過替代人員提供產品/服務並履行其義務。災難復原計劃（Disaster Recovery Plan）必須在 Citi 與供應商之間簽訂每個工作單（Work Order）之生效日起的十（10）個日曆天內提供給 Citi，此後，只要每個工作單有效，則每年提供一次。在供應商啟用其災難復原計劃時，供應商將向 Citi 提供必要的任何指示或其他資訊，以便 Citi 能繼續從供應商處獲得產品/服務。供應商表示、保證和承諾其災難復原計劃將至少包括：

1. 為了消除中斷的影響，包括無法取得技術（拒絕服務（DoS））、無法使用主要工作地點（禁止進入（DoA））和無員工（包括分包商）的復原流程和策略（包括遷移、工作轉移和/或遠端存取）；
2. 由供應商（包括但不限於）維護的與服務地點分開的第二個災難復原據點，與產品/服務地點分開的儲存備份媒體的地點，使用備援通訊線路和伺服器；
3. 產品/服務之操作和應用的備份/復原程序，包括一份詳細的書面計劃文件（其中包括在雙方同意的時間內恢復運作的流程和程序），以應對因電源故障、系統故障、天然災害或其他不可預見的情況而導致的長時間產品/服務中斷；
4. 保護所有內容的程序；
5. 供更換設備（例如電腦設備）的程序和任何第三方協議；

6. 供任何異地生產設施使用的程序；以及
7. 供應商的災難復原計劃將要求：
 - a. 對於任何可能對產品/服務造成負面影響的災難，供應商應立即通知 Citi ；
 - b. 供應商將在上述通知後的 24 小時內，向 Citi 提供可持續在備用處理設施提供產品/服務的計劃；
 - c. 產品/服務必須在要求的復原時間目標（RTO）內全面運作，除非在相關合約中另行定義，否則被 Citi 評為「企業關鍵性」或「高度」關鍵評級的流程為 4 小時或 4 小時以內；Citi 評為「中度」關鍵評級的流程是 24 小時或 24 小時以內；Citi 評為「低度」關鍵評級的流程是 72 小時或 72 小時以內；以及
 - d. 如果供應商部份的設施無法運作，供應商將以不亞於其對待其他商業顧客的待遇來對待 Citi 。

14.4 適用於託管服務的災難復原計劃規定

在供應商管理並為 Citi 提供提供託管服務的範圍內，以下條款也應適用。災難復原計劃至少包括：

1. 託管服務之運作和應用的備份/復原程序，包括一份詳細的書面計劃文件（其中包括在雙方同意的時間內恢復運作的流程和程序），以應對因電源故障、系統故障、自然災害或其他不可預見的情況而導致的長時間服務中斷；
2. 此外，供應商的災難復原計劃將要求：(a) 供應商將在發生任何可能對託管服務造成負面影響的災難後的二（2）小時內以書面通知 Citi；(b) 供應商將在此類通知的 24 小時內向 Citi 提供可持續在備用處理設施中提供此託管服務的計劃，以及 (c) 該託管服務必須在最初通知後的 48 小時內全面運作；
3. 供應商同意應要求發佈必要的資訊，讓 Citi 能夠建立災難復原計劃和業務連續性計劃，這些計劃將與供應商的災難復原計劃和業務連續性計劃同步運作；以及
4. 如果供應商部份的設施無法運作，供應商將以不亞於其對待其他商業顧客的待遇來對待 Citi 。

14.5 災難復原計劃的更改

供應商可更改其災難復原計劃，前提是，更改之後的災難復原計劃不可對其服務造成不利影響（例如，延長了復原時間目標（RTO））。任何災難復原計劃的更改，供應商應及時告知 Citi 並應 Citi 要求下說明更改原因，以便 Citi 可充分瞭解和對於變更作出回應。

14.6 分包商災難復原計劃

供應商將確保供應商的任何分包商具備一與 Citi 對供應商規定一致的災難復原計劃及相關的業務連續性控管機制。供應商應對分包商進行適當的監督，包括定期審查此類控管機制與測試結果，並確保及時補救任何發現的落差。

14.7 災難復原計劃啟動和危機通知

出現以下情況時，供應商將立即通知 Citi 業務主要聯絡人：

1. 當供應商啟動其災難復原計劃時，以及；
2. 牽涉到任何不利於供應商或其分包商之危機、威脅、警告或網路事件時，合理認為這些會對提供給 Citi 的服務或產品造成負面影響。

14.8 測試

供應商的所有復原資源和計劃都必須在正式上線後 120 天內進行測試（如果應用程式被 Citi 分類為企業關鍵性，則為 90 天），並應每年（每 12 個月）至少測試一次。該測試應展現供應商之能力，符合向 Citi 交付所有產品及服務所需之復原服務水準。這些測試必須是全面性，且包括向 Citi 提供的完整服務範圍。供應商應於至少 30 個日曆天前，預先通知對 Citi 提供的產品/服務之復原測試。Citi 可參與或觀察供應商對 Citi 所使用的應用程式之復原測試，以確認該應用程式在復原環境中的業務功能。如果 Citi 希望參與，供應商將在測試前向 Citi 提供測試目標、測試計劃和連線到測試網站的程序。供應商將在完成每個測試後的十（10）個工作日內向 Citi 提供測試目標、測試計劃和測試結果的摘要，包括復原所需的時間及測試結果證據（例如，螢幕截圖）。

14.9 數量驗證

對於託管 Citi 分類為「企業關鍵性」應用程式的供應商必須證明正式上線環境中的交易量可在其 COB /災難復原環境中處理。Citi 與供應商必須對於進行驗證的方式達成共識。

14.10 使用 Citi 的系統提供服務

如果 Citi 或 Citi 的附屬公司要求，使用 Citi 系統的供應商將參與 Citi 的災難復原演練行動，Citi 將不支付任何費用或收費。

14.11 處理測試結果

如果供應商的任何測試結果顯示未能達到任何測試目標或任何適用的 RTO，則供應商將執行一項來源成因分析，並迅速修復任何發現的缺失。在這類修復行動完成後，供應商將於初次測試失敗後（或相關工作單中規定的期限）的一百二十（120）個日曆天內（如果是 Citi 分類為企業關鍵性的應用程式，則為 90 個日曆天）再次測試。

14.12 危機管理

連同業務連續性計劃，供應商應具備一份對於復原操作的指揮及控管所需的危機管理計劃。供應商之危機管理計劃至少應指出獲充分授權以啟動復原操作之特定人員，規定收集及散播危機資訊之通訊及呈報協定，並包括於發生危機時，與 Citi 溝通之通知及呈報協定。

14.13 業務連續性評估

供應商必須遵守 Citi 第三方業務連續性評估流程，以評估供應商對於遵守 Citi 要求所採用的政策、程序及控管，以及與業務連續性相關的任何法律和/或法規要求（適用於 Citi 或供應商）。評估包括要求供應商回答的問卷以及佐證證據，同時還可能包括對供應商地點的訪問。如果評估結果揭露或顯示有問題或疑慮，Citi 將記錄所發現的問題或疑慮，並與供應商協力找出更正問題的方法。供應商應盡快進行必要之糾正措施及/或增加補強性控管機制，以解決 Citi 疑慮直到 Citi 合理滿意為止。

14.14 營運韌性

關鍵業務服務是指如果服務的交付中斷則可能會對 Citi、Citi 的客戶或金融系統造成重大負面衝擊的服務。供應商應確保，對服務要素的交付之任何中斷，無論是構成關鍵業務服務或支援 Citi 不時指示的 Citi 所提供的關鍵業務服務（以下稱「關鍵業務服務」）皆不超過 Citi 所設的持續時間或以其他方式違反 Citi 所設的任何相關指標（以下稱「衝擊容忍度」），供應商將不時接獲設定此容忍度的通知。「衝擊容忍度」將以明確的時間限制指標表示，相當於服務交付可能會中斷的時間期限。Citi 和供應商應每年審查「衝擊容忍度」作為持續性合約治理流程的項目之一。如果由於不止一個監管機構的規定造成 Citi 必須為個別關鍵業務服務設定一個以上衝擊容忍度時，Citi 得為此類關鍵業務服務指定單獨的衝擊容忍度。供應商應：

1. 在發現未能（或合理可能未能）在 Citi 所設的相應衝擊容忍度範圍內提供任何服務時，應立即通知 Citi，並解釋任可能的失敗原因或實際失敗原因，以及為消除此類失敗的影響而採取的措施；
2. 根據規定向 Citi 提供合理協助，以便 Citi 能夠識別供應商為提供關鍵業務服務所需要的人員、流程、技術、設施和資訊；
3. 向 Citi 提供合理協助，以便 Citi 執行：
 - a. 任何內部情境測試，測試在 Citi 或供應商的營運發生嚴重但可能會發生的中斷時，供應商是否有能力維持在每個關鍵業務服務的衝擊容忍度範圍內；以及
 - b. 在情境測試後演練從中吸取的任何教訓，使 Citi 能夠發現弱點和任何必要的行動，以改善供應商在未來中斷中有效應對和復原的能力。

如果 Citi 的任何內部情境測試發現供應商在 Citi 所設的相應衝擊容忍度範圍內提供服務的能力存在漏洞或缺陷，並且供應商未能在相應的衝擊容忍度範圍內提供任何服務時，雙方將協商出彼此同意的計劃（包括實施該計劃的時間表），以確保供應商採取必要的步驟來解決或消除此類漏洞或缺陷，或糾正造成失敗的原因，以便在合理可行的情況下盡快恢復到在衝擊容忍度範圍內（如適用）。

14.15 代管安排

在 Citi 要求下，(i) 向 Citi 授權軟體使用權以供在 Citi 環境內運作或 (ii) 向 Citi 提供託管服務的供應商應確保儲放材料（Deposit Materials）儲放在 Citi 指定的代管人處並簽署儲放人註冊表或代管人根據相關代管協議有關此儲放材料所要求的其他表格。在此之後，在與此項授權或託管服務相關的協議期的接下來時間中，供應商將向代管人儲放此儲放材料的最新版本，以確保代管的原始碼和其他儲放材料與適用於 Citi 所使用的軟體版本或託

管服務的軟體版本皆是最新版本。原始碼或其他儲放材料更新應在對授權給 Citi 的軟體或 Citi 所使用之託管服務修訂後三十（30）天內發送給代管人。供應商將完全遵守代管協議中載明關於儲放人的所有義務與要求。對於代管人所有的開支及費用，供應商將全權負責，包括但不限於設定費、年費、儲放費、服務費和任何其他的代管人費用和開支。在出現釋出事件時，代管人應根據相關協議和代管人協議的條款，向 Citi 或 Citi 的指定代表釋放此儲放材料。

如果原始碼（或其他儲放材料）是交付給 Citi 或 Citi 的指定代表（無論是由供應商直接交付或由代管人履行相關的代管人協議中的義務所交付），則原始碼和儲放材料必須遵守供應商和 Citi 之間相關協議下的現有授權規定；前提是，每個授權均被視為 Citi 有權在合理需要時使用和修改原始碼和其他儲放材料，以便：(i) 將軟體及其他儲放材料與 Citi 系統進行整合並確保其相容性；(ii) 使該軟體或其他儲放材料符合相關法律、產業標準或市場做法；(iii) 使該軟體或其他儲放材料與最新的技術創新同步，以及 (iv) 使該軟體和其他儲放材料在現有授權範圍內達成 Citi 及其附屬公司的業務目的。此軟體的任何版本，包括由 Citi 或代表 Citi 使用原始碼所開發之修訂版本，均受本節中所有條款及此主要協議約束；但是前提是，供應商將沒有此修訂版的權利、法定權利或利益，且任何修訂版的所有智慧財產權均歸 Citi。

供應商將與提供本軟體中所使用的任何軟體的第三方，共同竭盡商業上的合理努力，以允許供應商將此類第三方軟體的原始碼置於原始碼儲放中。如果第三方拒絕授予供應商此權利，則供應商應竭盡商業上合理的努力，以便在釋出事件後將相關的第三方軟體授權協議轉移至 Citi。

根據本節交付給 Citi 的原始碼應受相關授權軟體或託管服務的現有授權約束，前提是 Citi 可根據其業務和營運要求使用並修改原始碼和軟體，以讓此軟體與最新技術創新同步，並符合相關法律的要求。此軟體的任何版本，包括由 Citi 或代表 Citi 使用原始碼所開發之修訂版本，均受相關協議中所有條款約束；但是前提是，供應商將沒有此修訂版的權利、法定權利或利益，且任何修訂版的所有智慧財產權均歸 Citi。

15 全球背景篩查標準

適用於向 Citi 提供服務的所有第三方供應商。

15.1 總覽-背景篩查

背景篩查必須遵守所有當地的相關法律及法規。本文件中描述之所有資訊及自行披露內容皆應由供應商代表、供應商人員，及分包商酌情提供。根據當地法律，無論在履歷表上、面試中、入職表上還是入職流程中，無論何時遭發現偽造或遺漏資訊，將可能構成 Citi 拒絕或終止工作指派的理由。根據當地法律，無論何時遭發現所執行之篩查有不利結果時，亦可能構成 Citi 拒絕或終止工作指派的理由。

有關背景篩查完成的其他資訊，請瀏覽：

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

15.2 收集基本資訊和身份驗證

任何供應商人員在開始執行 Citi 任務之前，供應商應取得該人員之姓名、郵寄地址及永久地址（若不同）、電話號碼及電子郵件地址（若適用）。供應商人員也必須提供能證實其身份的文件。這可能包括提供國民身份證號碼、政府核發附有照片之身份證，或護照之資訊和/或證明文件。

15.3 制裁篩查

所有代表 Citi 執行工作或擁有 Citi 供應商股權至少 25% 的業主的供應商人員（包括分包商，且不論是否能存取 Citi 資料/系統/網路及/或進入 Citi 場所）皆應接受篩查，以確保未列於美國財政部外國資產控制辦公室（Office of Foreign Assets Control，簡稱「OFAC」）之《特別指定國民和被封鎖人員》（Specially Designated Nationals and Blocked Persons），簡稱「SDN」）及受美國制裁的地區及司法管轄區（「美國制裁」）等的名單中，以及美國以外政府當局發佈的任何制裁名單和受制裁的司法管轄區名稱，這些美國以外的政府當局發佈的名單及名稱包括歐盟（EU）的綜合金融制裁名單、聯合國（UN）安全理事會綜合名單、英國（UK）制裁名單以及根據適用於當地司法管轄區（「非美國的制裁」）的法律與法規列出的名單。

OFAC 名單可於本網站公開查閱：<https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 移民合規

供應商必須證明其具備相關規程並如實執行，以確認所有人員均已獲授權在其派駐國家工作。此外，供應商還必須：(1) 確保所有人員皆得到工作授權，以及 (2) 切實遵守所有適用法律、法規及政策（包括就業資格及驗證要求）。供應商亦應進一步證明已具備相關規程，確保其人員遵守所有適用之移民法律和法規，且該員對其所從事之工作及活動持有適當的簽證身份/類別。

15.5 工作經歷

供應商必須查驗其人員過去七（7）年或如果當地法規要求，十（10）年之工作經歷。此位人士的工作經歷必須接受查驗，以確保此人所提出的僱主、職位、日期及職務皆屬實。供應商人員還必須披露，過去曾於 Citi 或 Citi 任何前身公司（包括但不限於：Citibank、Citicorp、Travelers、Salomon Brothers 及/或 Smith Barney）擔任顧問或臨時員工之任何工作或任務。

15.6 教育背景

供應商必須查證其人員之最高學歷。驗證的資訊應包括入學日期、學校名稱、地址及取得的學位。

15.7 犯罪背景

在法律允許的情況下，供應商的人員及分包商如果因為任何刑事犯罪而成為逮捕、傳喚、傳訊、提訊、起訴或定罪之對象，包括認罪答辯或拒絕答辯，以及參與任何審前轉化程

序或類似程序，則該供應商人員及分包商必須向 Citi 披露。於法律允許且適用下，刑事記錄和/或指紋檢查之行政審核應於指派工作開始日期前完成。除法律另有禁止外，已定罪之盜竊、詐欺、不誠實、背信犯罪或當地不同法律定義的類似刑事犯罪皆可使 Citi 拒絕對其指派工作和/或不符合 Citi 指派工作的資格。根據適用當地法律和法規，其他定罪可導致 Citi 拒絕對其指派工作和/或不符合 Citi 指派工作的資格。

15.8 重新篩查

指派工作已結束之供應商人員，若再次由 Citi 指派工作時必須再次接受篩查。有關重新篩查要求的其他資訊，請參閱：

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

15.9 國際調職

所有篩查皆必須按照指派工作所在國家之法規完成。若供應商人員調職至新的國家，則此位人員應按照新國家之規定重新接受篩查。

16 開支

因合約原因而有資格申請業務開支報銷的供應商。

16.1 概覽

Citi 僅接受與業務相關且已獲得 Citi 事先書面核准的合理開支的報銷；且這些開支是供應商在向 Citi 提供產品及服務的過程中發生並符合相關合約的條款或 Citi 經營費用管理政策及其相關標準與程序（如適用），同時用來證明的收據、發票、行程或 Citi 認可的其他形式的文件可充分為憑。

16.2 開支報銷

此類開支應根據 Citi 之發票規定，妥善記錄並向 Citi 開具發票。供應商開支不得由 Citi 員工代表供應商產生此類開支。任何向 Citi 提交報銷的開支都必須是有效且經核准之費用項目，並且必須包括（除了所有其他發票規定之外）：

1. 費用的業務目的；
2. 費用金額及說明；
3. 費用產生的地點及日期；
4. 供應商提供服務之專案名稱/說明；
5. 要求提供此服務而產生此筆費用之 Citi 代表的姓名及業務關係；
6. 採購訂單號碼（如適用）。

有關可報銷的業務開支詳情，請聯絡您的 Citi 業務主要聯絡人。用作證明的收據、發票、行程或 Citi 認可的其他形式的文件必須隨附於提交的報銷申請中。報銷申請必須符合相關合約的條款或 Citi 經營費用管理政策及其相關標準及流程（如適用），並得到適當的業務發起人和/或 Citi 主要業務聯絡人的核准，以及由得到正式授權並具備購買相關商品足夠金額的人士核准。不符合規定者將不予報銷。

17 資安 (IS)

適用於可存取、處理、儲存或管理附錄中所分類和定義的任何 Citi 資訊的供應商（包括分包商）；或託管 Citi 品牌網際網路對向的應用程式，或可連結至 Citi 的網絡資源，或要求無需陪同自行進入 Citi 設施等的供應商（包括分包商）。

17.1 概覽

本節規定了 Citi 供應商（包括儲存、處理、管理或存取 Citi 資訊或託管 Citi 應用程式的供應商的分包處理商或分包商）或與 Citi 有網路連接的供應商在資訊保護控制方面的最低要求。這些要求確保資訊是根據 Citi 及其供應商營業所在地之適用法律及法規要求，以及最高產業標準（例如 ISO/IEC 27001/2）進行保護。若當地法律、法規或相關產業規範有較本文更嚴格之標準，供應商應遵守該等法律、法規或規範。此外，供應商可能被要求要納入額外的資安措施及程序，作為其遵守其他 Citi 政策及合約條款與條件之一部分。若供應商決定為資安實施額外的安全措施或程序，則供應商應確保此類措施及程序不與本節定義之最低控管相衝突。

17.2 資安政策與治理

供應商應有書面的資安政策及標準。政策治理必須包括定義明確的職務和責任，以及政策和標準年度審查/更新，以符合當前的技術狀態、產業標準、法律和監管要求。

17.3 責任分工

供應商應設立相關程序，確保對同一活動具有永久存取權限的個人不得執行任意兩個業務職能或兩個 IT 職能或兩個受控資訊系統職能，不得更改受控資訊系統或進行未經授權或檢測之交易，除非有足夠之補償機制用以降低風險。

一覽表 A

職能	職能說明
開發/工程	軟體、硬體、配置等的設計、建立或修改；範例可包括： - 設計並建立新的應用程式代碼和相關資料庫方案 - 策劃基礎設施產品和應用組件 - 客製化技術產品，以整合至軟體和服務

核准	核准將實施的程式碼變更升級
執行/管理系統	軟體、硬體、配置等變更的安裝、部署、或管理。範例包括： - 對生產基礎設施執行自動或手動程式碼發佈 - 安裝技術產品或電器 - 啟動或停止服務以支援有生產資料的系統疑難排解及補救措施
審查特權身份的活動	對於變更管理活動或與安全相關的系統事件（例如稽核追蹤）等的驗證
管理 ID	新增 ID（使用者、FID 和機器人）及其修改和刪除，權限或密碼
業務職能	職能說明
啟動業務交易	啟動（也稱輸入或建立）業務交易及變更顧客資訊
核准業務交易	核准（也稱為授權或檢查或發佈）業務交易
IT 職能	職能說明
網路運作	提供網路基礎設施服務的產品的裝置管理和運作支援。範例包括：網路路由器、交換機、防火牆、網域名稱服務（DNS）
非網路運作	對不提供網路基礎設施服務的產品的裝置管理和運作支援。範例包括伺服器、手機和電腦

17.4 管理層對資安的承諾

將託管 Citi 品牌網際網路應用程式及/或有權存取分類為機密或更高層級 Citi 資訊的供應商須遵守 Citi 的第三方資安評估流程（TPISA），評估供應商之政策、程序及控管是否符合 Citi 規定，以及關於資安之任何相關法律和/或法規要求（適用於 Citi 或供應商）。

評估包括需要供應商回答的資安問卷以及佐證證明，同時還可包括對第三方儲存、處理、管理或存取 Citi 機密或更高層級資訊的供應商地點的訪問。此外，TPISA 第三方連續監控團隊可能會使用網路安全監控工具監控供應商，這些工具可利用公開可取得的資訊以針對生命週期結束軟體、存在漏洞的開放連接埠、易遭受攻擊性或其他外洩情況等來找出具有這些風險的對外網際網路系統、主機、應用程式和伺服器。若 TPISA 監控結果發現或顯示有資安問題或疑慮，則 Citi 會將所發現的結果予以記錄並通知供應商，以與供應商協力找出解決此問題的方法。在 Citi 全權斟酌決定下，供應商必須盡快進行必要之糾正措施以增加/或補強控管機制解決 Citi 的疑慮，同時還要滿足以下各種問題所規定的解決期限，包括高風險問題 180 個日曆天、中度風險問題 240 個日曆天、低風險問題在下一合規日期前，因為這些問題都是 Citi 所作出的評級。

1. 供應商必須根據自己在資安方面的標準、政策和程序，定期對其業務營運和相關控管進行評估。定期評估應至少包括：
 - a) 評估供應商所用之程序，確保是否符合供應商自己的資安政策及標準；
 - b) 評估輔助資源，例如供應商所用之應用程式及基礎設施，以及支援供應商業務營運之分包商（如適用）所用之資安事件流程，或亦可允許 Citi 執行該類評估。若第三方與分包商簽定可存取、處理、管理或處置被分類為機密或更高層級 Citi 資訊之新合約或延續現有合約時，必須遵守相關法規。
2. 凡經過資安風險評估（即 TPISA）後所發現之問題皆應記錄在案，並追蹤至結案為止，且將修復之證據提供給 Citi。
3. 若供應商之資安管理職能部門遷移至國外，供應商應於事前取得 Citi 書面核准。
4. 如果供應商收購新法人，供應商必須完成對被收購法人的評估，以確保其符合這些標準。
5. 除非獲得 Citi 事先書面核准，否則供應商不得外包用以儲存、處理和/或傳輸 Citi 資訊之系統的安全管理職能，包括但不限於防火牆管理、安全配置管理、修補管理或資安管理（ISA）職能。
6. 如果供應商管理的軟體或網站中包含 Citi 資訊或屬 Citi 品牌，則必須根據 Citi 的系統安全測試標準（SSTS）進行定期漏洞評估，且在評估中發現的任何重大問題都必須於此標準所規定的期間內予以修復。由於 SSTS 未被核准對外分發，供應商必須與其 Citi 關係經理合作，以確保遵守這些參考文件。此外，供應商必須遵守相關的 ISO/IEC 27001 資安管理標準（或建立更高標準和協定的接續的資安管理標準），並遵守本第（17）節中的資安規定。
7. 若需要連線至 Citi 內部網路之伺服器及/或資訊系統，供應商應通知其 Citi 業務主要聯絡人，以便遵循目前的連線配置程序。
8. 如有任何擅自存取 Citi 資訊，或獲取、遺失、破壞或刪除 Citi 資訊，或用以儲存、處理或傳輸 Citi 資訊之資訊系統遭到任何其他損壞，供應商應立即通知適當之 Citi 聯絡人（業務活動負責人，即 BAO）。
9. 供應商必須確保所有高風險活動或敏感資料的變更皆具備稽核追蹤記錄，以便追蹤這些操作至其執行人士。
10. 供應商必須確保在電腦螢幕或紙張（包括例如監控、例外情況及監管，以及其他報告）上的所有機密或更高層級的資料皆進行遮罩。

11. 供應商必須限制對於敏感資料進行列印、錄製或複印，包括透過自己的裝置進行這些操作。協議期間或協議結束時，供應商應歸還或銷毀所有 Citi 資訊，除非法律或法規禁止。
12. 供應商必須確保可存取 Citi 資訊的供應商所有人員（員工、承包商、臨時員工、分包商）都簽署保密協議或機密協議。
13. 供應商必須為其員工提供員工手冊或類似文件，這些文件中包含違反供應商行為指導方針的懲處流程，以及員工入職流程中所必須確認的人力資源政策。
14. 當員工或非員工被解僱或辭職時，供應商設有適當的流程以取回所有資產。
15. 如果供應商保有任何機密資訊或以任何方式儲存於網站或網路可存取的系統上，供應商必須向 Citi 披露此資訊。此項披露可包括在服務說明中。如果供應商持有或儲存 Citi 機密資訊，供應商將在本協議期限內每年執行一次 SSAE 18 稽核（或任何 Citi 核准的接續的權威評估），並且將每年不少於一次向 Citi 提供記錄此 SSAE 18 稽核結果的報告或 Citi 核准的任何接續的權威評估結果的報告。
16. 如果在任何合併或收購或類似交易中，供應商被收購或收購另一法人，且此類交易可能會影響服務時，供應商必須立即以書面通知 Citi，且供應商必須按照此處的規定對此項交易結果的法人進行資安評估，以確保此項合併或收購不會影響對這些要求的合規性。

17.5 分包商資安風險

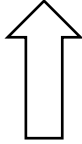
供應商必須要求可存取 Citi 機密或更高層級資料的分包商接受由合格的資安人員執行的合約前資安（IS）評估及合約後的定期資安評估。這些評估應根據管理層核准的流程以處理從啟動到問題管理的所有階段的流程執行。分包商 IS 評估應使用一份問卷或等效工具，評估 IS 網域內的分包商風險狀況是否符合 Citi 的第三方 IS 評估問卷（TPAQ）中所包含的 IS 評估網域內的分包商風險狀況，並且應包括計算與分包商參與相關 IS 風險的邏輯方法。供應商必須追蹤評估完成的狀態並管理發現的問題及糾正行動計劃以結案。

17.6 資產責任

1. 供應商應確保隨時更新在其控制之下，維護用於儲存、處理和/或傳輸 Citi 資訊之所有應用程式以及硬體之庫存清單。
2. 供應商應確保能夠根據可適當維護該清單之準確性及完整性的流程，維護在其控制之下的 Citi 資訊資產清單。
3. 供應商應負責保護其控制下之所有 Citi 資訊。
4. 供應商應以符合產業做法的方式確保承擔起其使用者活動之責任。
5. Citi 資訊所在之供應商全球網路，應限制使用者存取個人外部網際網路電子郵件之儲存空間帳戶及雲端儲存空間帳戶。

17.7 資訊分類和處理

Citi 按以下資訊分類表進行資訊分類：請參閱附錄以瞭解下列每個資訊分類的定義和範例。

限制性	最敏感
敏感 PII	
機密 PII	
機密	
內部 PII	
內部	
公開	最不敏感

1. 按照 Citi 資訊分類，Citi 必須與供應商合作共同具體規定保護該資訊所需之安全層級，且供應商必須確保實施充分之控管，以及任何 Citi 可能隨後需要升高或修改之層級。
2. 內部或更高層級的資訊必須儲存於符合第三方與 Citi 之間合約規定的第三方託管裝置，且該項合約中包含符合 Citi 政策及標準的機密性條款。
3. 如果供應商允許使用非公司所擁有的裝置儲存 Citi 資訊（即，由第四方託管的裝置），則供應商應設有規定特定管理層核准的政策，並制定使用及處置 Citi 資訊的指導原則及監控流程。
4. 供應商應始終保護 Citi 資訊，讓其免遭未授權存取、修改或刪除。
5. 透過可攜式電子媒體（ETM）傳輸、分類為機密或更高層級的 Citi 資訊必須使用核准的加密演算法進行加密，且必須確認傳送。供應商必須確認指定的收件人已收到 ETM。若直至預訂交付日期仍未收到確認收件通知，供應商必須通知 Citi。

17.8 安全配置

1. 供應商必須對可能儲存、處理、存取或傳輸 Citi 資訊的所有資產提供明文規定的安全配置標準。
2. 供應商必須將資安控管整合至其應用程式、產品及服務的選擇、開發及實施流程及程序中。
3. 供應商應具備安全組建程序，供所有儲存、處理和/或傳輸 Citi 資訊之所有系統使用。
4. 供應商必須具備所有系統的安全圖像或範本。
5. 所有預設的使用者帳戶及密碼都必須從供應商支援的系統、網路裝置及應用程式中移除及/或變更。
6. 任何被入侵的系統或服務都必須使用經驗證為完整的圖片或範本重新建立及配置。
7. 對安全配置所進行的任何變更皆必須透過供應商變更管理流程由管理層核准。
8. 供應商必須通知 Citi 任何安全配置的變更。
9. 安全組建程序應包含能夠在正式上線部署時支援安全/標準組建設定之自動化配置檢查工具，以及對於基準配置的合規及偏離之持續監控。

17.9 加密要求

供應商不得傳輸未加密的機密級或更高層級資訊。被分類為機密級或更高層級的資訊必須使用 Citi 核准的工具或解決方案進行點對點加密。經核准可供資料加密傳輸的協定和相關版本號碼如下：

1. 供傳輸認證資訊和授權資訊：SAML v2.0、OAuth v2.0（僅限授權）
2. 為保護通訊管道和相關的金鑰交換，我們僅允許以下的網路安全協定：
 - a) TLS v1.3 是首選的安全協定，因此允許所有的 TLS v1.3 套件。如果 TLS v1.3 是唯一啟用的協定，此時無需其他審查。
 - b) 如果 TLS v1.3 在技術上不可行且已使用了 TLS v1.2，此時便可接受 SSLLab 的 B 級或更高層級，且無需其他審查。

永久儲存在 Citi 第三方環境中或交換的資料，必須使用 Citi 核准的工具或解決方案完全加密。核准的加密資料演算法與金鑰的長度如下：

1. **進階加密標準（AES）**：核准的金鑰長度：256 位元或更多位元。限制性模式：禁止使用電子密碼本（ECB）模式，除非明文量小於或等於分組長度。磁碟驅動器加密：要求使用 256 位元金鑰的 AES。具有 128 位元金鑰長度的 AES 允許作為 TLS 密碼選項；但是，這些密碼將在 2028 年 12 月 31 日後被禁止，由 256 位元或更高強度的位元取代，以便讓 Citi 能夠與國際時間表同步（參考：NIST 8547 IPD）。
2. **ChaCha20（相關用例的串流加密）**：核准的金鑰長度：128 位元或 256 位元，具有 96 位元隨機數和 32 位元區塊計數或 64 位元隨機數和 64 位元區塊計數。最大資料大小：16 拍字節。

所核准的公共金鑰密碼系統、金鑰交換、協議機制、訊息摘要和金鑰衍生功能如下：

與供應商量子準備就緒相關的通知：供應商必須透過（[survey link](#)）向 Citi 量子準備就緒計劃團隊出示 NIST IR 8547（ipd）的表 2 及表 4 計劃。

1. **公共金鑰密碼系統和最小金鑰長度大小**：
 - a) RSA 加密演算法（RSA）：2048 位元。
 - b) 數位簽章演算法（DSA）：2048 位元。DSA 不得用於保護在 Citi 之外處理或儲存的 Citi 資料。
 - c) 橢圓曲線數位簽章演算法（ECDSA）：256 位元，並按照 ANSI X9.62 的規範及 NIST 推薦的曲線進行。
2. **金鑰交換和協議機制以及最小金鑰長度大小**：
 - a) Diffie-Hellman（DH） / Ephemeral Diffie-Hellman（DHE）：2048 位元。
 - b) Elliptic-curve Diffie-Hellman（ECDH） / Ephemeral Elliptic-curve Diffie-Hellman（ECDHE）：256 位元，並按照 ANSI X9.63 的規範及 NIST 推薦的曲線進行。¹
3. **訊息摘要功能**：禁止建立長度大於用於產生哈希的材料中隨機位元數的加密金鑰。

¹ 最好使用 ECDHE。

- a) SHA-1 僅適用於非數位簽章應用程式。SHA-2 系列、SHA-3 系列和 POLY-1305：可用於所有加密哈希函數應用程式。

4. 基於金鑰衍生函數的密碼和最低要求：

- a) PBKDF2：迭代次數至少為 10000 次，且鹽值長度至少 16 位元。
- b) HKDF：必須加入 Salt（隨機鹽值），並且必須包含資訊輸入值。
- c) SCRYPT：最少回合數/成本因子為 10。
- d) 禁止使用 NIST SP800-108 KDF 進行串流加密。可使用 NIST SP 800-108 KDF 模式，即計數器、回饋意見和雙支持管道迭代模式。
- e) 建議使用 Argon2。

5. 密碼哈希函數和最低要求：

- a) Bcrypt（用於本機儲存的驗證資料）：最少回合數/成本因子至少為 10。
- b) 在將密碼儲存於任部署在環境或系統中任何供應商的本機產品時，對於密碼雜湊建議使用 Argon2 或 PBKDF2。

17.10 外部電子郵件

若法規和/或供應商政策不允許供應商使用 Citi 核准之端對端加密軟體或工具，則含有機密級或更高層級的 Citi 資訊之個人電子郵件，得透過傳輸加密（例如，透過傳輸層安全協議（TLS）之閘道器對閘道器加密），以完全滿足加密要求。經核准的安全電子郵件協定是：

1. 基於身份的加密（IBE）具有加密電子郵件的功能，並且只能在可用於 Citi 顧客的解決方案及安全電子郵件與 eDelivery 系統中使用。
2. 強制 TLS（MTLS）具有工作階段加密的功能（不會加密電子郵件內容），並且供已預先協商好使用方式的供應商、合作夥伴及客戶使用。
3. 域名金鑰辨識郵件（DKIM）具有來源驗證及金鑰管理功能，並可與供應商、合作夥伴及客戶使用。

17.11 私人網路

私人網路若受認可機構獨立監督，且符合用於授權或正式認可之對手方（例如 SWIFT 或中央銀行）之間，處理交易業務之金融服務產業規範則可考慮豁免機密 PII 傳輸加密要求，直至該類網路提供必要之基礎設施可完全支援加密傳輸為止。

17.12 語音及傳真

透過傳真發送或語音通話（包括網際協議通話技術 [VOIP]）中討論 Citi 機密或更高層級資訊可不加密發送。若有需要，供應商應制定具體程序及指引以保護透過此類管道發送之機密或更高層級資訊。

17.13 加密金鑰及憑證管理

本節使用的安全邊界一詞是指加密模組驗證計劃（CMVP），例如聯邦資訊保護標準（FIPS）、驗證邊界（FIPS 140-2/3 第 2 級是可接受的最低安全層級）。（可接受例如 AWS Nitro Enclaves 之類的機密運算記憶體位置。其他獨特的安全邊界案件必須經過 Citi 核准）。

1. 供應商必須部署目前業界標準的加密演算法，且為加密及簽章維持最小金鑰長度（包括 **SSH** 金鑰）。當此類演算法及金鑰長度為了符合產業標準而進行更新時，供應商必須透過其「變更管理流程」提供保證。
2. 供應商必須具備正式記錄的金鑰、機密資訊、憑證管理生命週期流程，並採取適當的控管機制來保護敏感資料免遭未經授權的使用或洩露。所有加密機密及金鑰生命週期事件都必須僅在安全範圍內發生。所有對於特權和安全邊界的存取權限都必須記錄。供應商必須為所有金鑰生命週期事件提供序列圖，以突顯所涉及的角色、實體和邊界。
3. 加密金鑰必須具有一個唯一的目的，並且絕不得用於任何其他目的，例如使用相同的加密金鑰進行磁碟加密，以及資料加密，或使用相同的加密金鑰進行承載加密以及資料庫加密。**SaaS** 供應商將加密金鑰重複使用多個租戶被預設為禁止，且僅允許案件是涉及被分類為機密 **PII**、敏感 **PII** 和限制級 **Citi** 資訊的非關鍵、低風險所使用，同時還必須明確得到安全架構委員會的核准。
4. 對於所有加密金鑰（無論是對稱或不對稱），私密金鑰或私密金鑰材料（例如種子，或私密金鑰的一部分）在任何時候都不得以明文形式顯示。除了動態工作階段金鑰等暫時性金鑰之外，私密金鑰或私密金鑰材料（例如種子或部分私密金鑰）絕不能離開安全邊界。如果設計要求對稱金鑰或私密金鑰或私密金鑰材料以便在安全的記憶體位址/特權存取邊界之間傳輸，則必須僅使用「對稱金鑰包裝金鑰」或「公開金鑰傳輸金鑰」透過共同 **TLS** 加密隧道進行加密形式傳輸，且此類傳輸必須獲得 **Citi** 的書面核准。私密金鑰傳輸金鑰絕不得離開在這些案件中產生的特權存取安全邊界。
5. 「對稱金鑰包裝金鑰」必須拆分為兩個或更多個金鑰元件，並在散發之前進行異或運算，以便進行手動輸入/載入金鑰。「對稱金鑰包裝金鑰」必須與安全邊界內部關聯的足夠的存取控制清單（**ACL**），例如 **CMVP** 驗證的模組，且此「對稱金鑰包裝金鑰」絕不得儲存於安全邊界之外。
6. 人為代理人或服務代理人或自動代理人等存取包含私密金鑰或密碼或私密金鑰材料（例如種子或部分私密金鑰）的金鑰庫或安全邊界必須進行適當的分隔，並透過控制措施，限制僅授權人員或系統的存取。
7. 對含有私密金鑰或對稱金鑰的金鑰庫，每一次的存取請求都必須登入與記錄，內容包括存取人員、存取時間和存取目的等詳細資訊，以供稽核之用。
8. 供應商不得使用自簽憑證及萬用字元憑證或預設 **SSL** 憑證。
9. 所有加密金鑰必須具有規定的加密有效期間長度，如 **NIST SP800-57** 第 1 部分第 6 修訂版中所建議。金鑰到期前必須先重新整理或迴轉以容納變更期間、排程衝突、系統凍結等情形。
 - a) 在更換過期憑證時，禁止再度使用舊的非對稱金鑰對。
10. 加密金鑰的完整性、金鑰儲存或分享的媒體，或疑似對稱或私密金鑰的機密性遭到破壞時，金鑰必須立即被視為遭到破壞。所有遭到破壞的金鑰都必須從操作使用中移除，且所有相應的憑證也必須取消。
11. 應使用產業規範之加密演算法，對無線網路進行加密。
12. 供應商使用任何形式之加密機制時，應使用產業規範之金鑰管理工具及技術。金鑰管理職務必須與經營管理職務分開。

13. 供應商僅在確保與 Citi 資料安全服務提供的 PKI & KMS 服務具有互用性，且未將加密控管委託給 Citi 以外的加密治理時，才可使用雲端原生 KMS 和 PKI。

17.14 存取權控管責任

為了保護所有用來儲存、存取、管理、處理或傳輸 Citi 機密或更高層級資訊的「受管制資訊系統」免於被擅自存取，供應商有責任執行最低權限原則，即將使用者權限限制至每個工作職能所需的最低權限層級，以及管理對所有系統及應用程式的邏輯存取權限之提供。控管措施必須有完整記錄且可進行稽核。存取權限的授權和取消授權，包括密碼重設及啟用，在盡可能的情況下必須透過自動化程序執行，以確保風險緩解，避免因人為錯誤導致的過度授權，並符合產業標準。

1. 供應商應負責其組織內所有使用者之存取權。
2. 供應商應實施存取控制，嚴格確保僅授予使用者實施其職能所需的權限及權利。
3. 供應商應實施相關流程，確保所有預設存取功能已移除、停用或受保護，以避免遭到擅自使用。

17.15 使用者存取權限管理

供應商必須管理用來處理、儲存及/或傳輸 Citi 機密或更高層級資訊的系統及應用程式的邏輯存取權限之提供。這包括：

1. 識別及庫存清點已核准的驗證系統。
2. 規定所有對於 Citi 資訊的存取權限都需要主管或主管的指定代表及系統所有人核准。供應商必須負責確保其公司中任何可存取 Citi 資料的人員是基於需要知道才能被授予此類存取權限。
3. 規定如果可能造成利益衝突或違反經辦與覆核（maker-checker）規則，則不得對個人使用者提供任何特殊存取權及職能的組合。
4. 一個監督及管理授予/撤銷系統中每位使用者存取權的監控流程。
5. 存取權請求不得使用鏡像或複製另一位使用者的權限；請求人應說明明確的職務/權限以及業務理由以防止權限蔓延並強制執行最小權限原則。

17.16 使用者識別和身份驗證

所有供應商控管之資訊系統，應驗證存取此平台之使用者或系統，才能啟動存取 Citi 資訊的工作階段或操作。

1. 使用者必須透過使用者 ID，進行唯一的身份識別或對應才可登入技術平台。
2. 使用者必須使用核准的驗證方式在技術平台上進行驗證-供應商應聯絡其業務主要聯絡人（業務活動負責人，即 BAO），以瞭解目前核准的方式。

3. 共用身份驗證基礎設施之所有使用（例如，單一登入、減少登入次數或其他共用身份驗證之服務）皆應符合 Citi 身份驗證要求。供應商應聯絡其主要業務負責人（業務活動負責人，即 BAO），以瞭解目前核准之方式。
4. 用於在資訊系統中驗證使用者身份之身份驗證資料（IVD）在傳輸及儲存時進行加密。請參閱第 17.9 節的加密要求。
5. 供應商人員用來存取 Citi 系統的每個帳戶都必須對應至 Citi 指定的唯一識別碼（例如 GEID）；禁止使用通用/共享的使用者 ID 供人類使用者使用，以確保可進行追蹤、SOD 執行及接受稽核。

17.17 特權存取權身份識別和臨時特權存取權

供應商必須具備一份所有身份的清單，並識別出擁有特權存取權的身份，或有權存取包含被歸類為機密 PII 或更高層級資訊的電子儲存庫（支援業務應用程式的資料集或資料庫）的身份。供應商應實施防止未經授權使用這些身份的控管措施。如果員工需要使用到特權 ID 或之前提到的電子儲存庫，則必須透過以下的臨時存取管理流程授予存取權限：

1. 申請人應已在預先核准授權使用者名單上，或使用時取得核准。
2. 授予存取權限之前，應在變更/問題單上記錄理由。
3. 包括對於使用此存取權限執行的活動進行獨立審查。
4. 包括在臨時存取公佈期間結尾時所發起的撤銷/移除存取權限的流程。
5. 允許正式上線及實施後穩定存取（例如重大升級或間斷/修復解決方案後）最多延長七（7）個日曆天。

17.18 使用者存取權之審核

1. 供應商應至少每半年一次實施明文規定之流程，以審查、驗證及刪除儲存、處理、管理和/或傳輸 Citi 資訊之管制資訊系統中不必要的使用者權限。
2. 使用者不得審查或核准自己的權限，或對其負審查責任之人的權限。
3. 在可存取 Citi 資訊的供應商人員職能變動之後，供應商可在 14 個日曆天內執行存取及權利審查，如果此員工的新職能不再需要存取 Citi 資訊，則可移除其存取權限。

17.19 安全登入程序

1. 帳號遭鎖住之使用者登入 ID 應透過產業規範重置服務或其他授權功能重新啟用。操作系統或應用程式支援的橫幅文字，必須顯示在使用者初始登入或被驗證的所有網路入口點。

17.20 密碼管理系統

1. 絕不能於螢幕上明文顯示使用者靜態密碼。如有顯示密碼切換功能可免除此要求，前提是：
 - (1) 密碼輸入被預設為遮蔽，
 - (2) 顯示密碼只能由明確的使用者操作啟動，
 - (3) 密碼在使用者動作中斷後最長 15 秒便將自動重新遮蔽。
2. 特權功能 ID 密碼不得以明文形式硬編碼。

3. 靜態密碼必須至少有十（10）個字元，其中應包含字母及數字且必須區分大小寫。每個驗證點都必須驗證靜態密碼的大小寫字母。對於 2026 年 8 月 31 日後推出的應用程式，功能 ID（FID）的靜態密碼必須包含至少 15 個字元。
4. 僅在需使用 PIN 以滿足實體裝置之限制時（例如，小鍵盤、電話、智慧卡），PIN 方可作為存取資訊系統時的唯一身份驗證方式。
5. 所有靜態密碼應至少每 90 個日曆天變更一次。
6. 所有靜態密碼在連續六（6）次登入失敗或連續六（6）次密碼重設失敗後必須鎖住。密碼必須透過 ID 管理員功能解鎖，或至少 30 分鐘後自動解鎖。
7. 所有身份驗證系統皆必須實施不超過 100 個日曆天的登入閒置/非使用狀態控管。如果技術上可行，被停用的帳戶得透過使用者或其他授權職能重新啟用。
8. 驗證程序必須確保相同的密碼在至少最後六（6）次的變更期間未曾使用過。

17.21 系統公用程式之使用

供應商應確保對於能夠覆蓋系統及應用控制（例如，從周邊裝置啟動）之公用程式的使用受到限制及控管。

17.22 工作階段逾時

1. 對於儲存、處理和/或傳輸 Citi 資訊之管制資訊系統之所有使用者，都應登入並且重新驗證。
2. 使用者於不超過 30 分鐘的閒置後，應重新驗證身份。活動包括端點（滑鼠、鍵盤、觸控式螢幕等）的任何輸入。受密碼保護之螢幕保護程式強制執行之情況不必使用應用程式/單一強制登入。

17.23 終止使用者存取權限

1. 使用者停職或辭職後，其允許存取 Citi 機密或更高層級資訊（包括使用者登入 Desktop/Active Directory、單一登入（SSO）、電子郵件、一次性密碼（OTP）權杖及遠端存取）的使用者存取權限或權利必須立即移除。
2. 如果員工可存取 Citi 擁有及管理的系統，則當該員工的職能變動或離職時，必須立即通知 Citi 業務關係經理、BAO 或 BAO 支援部門，以確保 Citi 業務經理在離職日結束前啟動對此離職員工的存取權限移除。
3. 供應商已備有明文規定流程，在員工或非員工被解僱或辭職時，根據第 17.23.2 節所載明的時間框架，取回所有資產中的存取權限。
4. 如果供應商發現任何有關 17.23.1 至 17.23.3 節的異常情況，供應商必須立即通知 Citi 業務關係經理、BAO 或 BAO 支援部門，並提供合理的理由和控管措施。

17.24 遠端存取

供應商必須設有遠端存取控管機制以保護對可儲存、處理、傳輸 Citi 機密或更高層級資料的網路之存取，這些控管機制包括：

1. 應保護儲存、處理、管理和/或傳輸 Citi 資訊之資訊系統的遠端存取權限，以免遭擅自使用。

2. 所有供應商管理的筆記型電腦及所有供應商管理的桌上型機器如用於儲存、處理及/或傳輸 Citi 資訊，並透過遠端存取在本機進行儲存/處理分類為機密或更高層級的 Citi 資訊，必須使用符合業界標準的加密工具進行加密。
3. 遠端連結僅可透過使用多因素驗證（MFA）且經過核准的遠端存取解決方案建立。
4. 供應商所管理之機器應安裝個人防火牆，並在直接連線網際網路時（即，並非透過供應商所管理之防火牆或代理伺服器）啟動。
5. 供應商管理的裝置必須定期連線至供應商網路以定期接收和安裝軟體/防毒工具之更新，以符合全面存取網路的規定。可基於更新裝置的明確目的而允許有限存取。
6. 如果使用非供應商所擁有及管理的裝置存取 Citi 機密或更高層級資訊，則裝置必須配置為使用經授權且不允許資訊下載至本機的解決方案。必須設有以下控管措施：
 - a) 防止將 Citi 資料下載至公司所管理的解決方案之外的裝置。
 - b) 供應商應確保使用標準遠端存取技術（例如虛擬桌面基礎結構，簡稱 VDI），透過權杖或憑證基礎之身份認證方法，以保護該類存取。
 - c) 必須配置 Terminal Services、VMware Horizon 等遠端存取解決方案以停用在 Blast、PCoIP 上的剪貼簿分享及硬碟映射功能，以及停用 RDP 及 SSH 協定。
7. 如果使用軟權杖進行 MFA，例如使用行動裝置上的軟體應用程式，則軟權杖認證軟體必須對使用者進行驗證（例如，透過密碼、生物特徵等），並在行動裝置被破解或刷機（使用行動裝置供應商所認證和提供的操作系統以外的操作系統）時防止其使用。
8. 所有供應商人員，包括但不限於永久員工/臨時僱員、承包商和分包商，需要對系統、資料儲存庫、應用程式及/或基礎設施有特殊存取權限、特權存取權限及/或管理層級的存取權限，包括但不限於直接或間接與為 Citi 提供的服務相關的系統管理員、資料庫管理員、存取控制管理員、防火牆管理員、網站管理員等，應僅使用多因素驗證程序（MFA）進行驗證。同時，此類存取權限將由供應商根據上文所述的規定單獨記錄和監控，以找出可疑活動及/或未經授權的存取行為。
9. 對於個人擁有的裝置和第三方擁有的裝置，供應商必須具備有效解決方案，以確保此類裝置在被允許登入網路之前已備有經核准的作業系統版本、修補級別、防病毒和反惡意軟體解決方案。
10. 供應商必須確保其所有人員將：
 - a) 具備一個不包含任何語音輔助裝置（例如 Alexa）、錄影裝置及/或任何其他照相、視訊或音訊收聽/錄音裝置的私人專用遠端工作空間。不允許未經授權的人員瀏覽可能出現在遠端電腦系統螢幕上的任何資料、系統、應用程式。
 - b) 在離開電腦時將電腦鎖住，以充分降低未經授權而進入電腦查看螢幕的可能性。

17.25 清桌政策

供應商人員應保護所有形式之 Citi 資訊，包括於工作場所使用或儲存之實體資訊。供應商必須每年至少一次，透過資安訓練或其他管道向其所有員工傳達此項規定。

17.26 消防安全

1. 供應商應遵守規範實體安全及建立安全工作環境適用的法律及法規規定，包括當地消防規範。
2. 供應商應使用火災探測、警報器及滅火系統。此系統應每半年檢查一次且每年測試一次。

17.27 實體安全性

1. Citi 資訊應儲存於設有出入控制、僅限獲授權人員存取之安全區域。
2. 供應商應實施明文規定且可供稽核之實體出入控管系統。
3. 供應商應對於所提供之環境及服務屬適當的情況下使用結合了安全警報/防止侵入系統的組合措施，其中包括第三方監視之安全警報、保全人員及視訊監控等。
4. 供應商應有明文規定之訪客政策，包括要求所有訪客於抵達及進出時，均要提供身份證明文件。

17.28 操作安全程序與責任

1. 供應商變更管理流程時必須包括針對變更註冊、審查、測試、核准、實施、關閉之關鍵檢查點控管。供應商還必須具備緊急變更流程，此流程需要列出關於包括強制核准等級制度的所有階段。
2. 供應商必須為能力管理制定可稽核的流程，包括（但不限於）可用性、能力及績效指標/指標；業務影響評估；主動追蹤、調查績效及處理績效與能力問題。
3. 如果適用，供應商應確保實驗室、開發、測試及正式上線等環境在實體上及/或邏輯上相互分開。

17.29 軟體開發規定

適用於所開發的軟體僅供 Citi 使用的供應商。供應商應遵循這些規定，或證明具備有完整記錄且經核准的軟體開發生命週期（SDLC）流程，並使用同等品質的等效方法。

17.30 啟動和規劃

供應商必須根據 Citi 的要求及合約義務，定義解決方案的範圍及目標。這包括：

1. 記錄功能性及非功能性要求；
2. 提供預計的工作量和時間；以及
3. 識別所有第三方的組成部分或依賴項。

合規活動（包括安全風險評估）都必須在專案開端時展開。職務、責任和核准等檢查點都必須清楚溝通。

所有環境都必須分類為開發（DEV）或測試（TEST）或正式上線（PROD），並在整個生命週期中嚴格分隔。環境分類決定存取權限以及可能處理的資料類型。供應商必須根據環境分類限制存取權，並將配置與適當的 SDLC 完成階段保持一致，以防止未經授權的存取或資料外洩。

17.31 設計

供應商必須記錄足以確保所交付的解決方案符合所有要求（即「測試計劃」）的設計方法。測試計劃必須至少包括以下各項並提供說明：

1. 開發團隊將執行的所有測試，包括單元測試和功能性及非功能性測試，以及性能方面的測試，並追溯至規定的要求；
2. 指定將負責確認完工的核准人；
3. 安全性測試要求，例如漏洞評估和威脅模型分析；以及
4. 測試的環境、方法、流程、推廣路徑。

發佈策略必須詳細說明發佈到 TEST 和 PROD 環境中的先決條件和流程，包括發佈已準備就緒的標準、內容和整個專案生命週期的交付步調。

如果合約中另有指定，軟體派送時必須使用 Citi 核准的工具及工作流程，以 Citi 核准的格式包裝。

17.32 測試

測試必須在控管環境中規劃和執行，以驗證該解決方案符合規定的要求及成功標準。測試用例必須能夠追溯到 Citi 要求及程式碼提交。

供應商應準備一份總結通過/失敗結果的報告、開發期間進行的額外測試，以及任何未完成測試（並提供原因）（即「測試結案報告」）。所有瑕疵和遞延的能力都必須記錄，以及未解決問題的緩解計劃。

應 Citi 要求下，供應商必須提供以下證據：

1. 詳細的測試計劃；
2. 「測試結案報告」中詳述測試完成及結果；以及
3. 測試結果可追溯至 Citi 要求與程式碼提交。

17.33 配置

在進行配置前，供應商必須完成所有規定的安全性測試，包括漏洞掃描及威脅模型分析。發佈流程必須有條理，包含變更記錄、復原策略和所需的核准等記錄。實施計劃與配置等操作手冊必須包括監控和向上呈報規程。

配置完成後，供應商必須確認系統身份識別資料並更新所有相關的工件，以確保可進行稽核。

17.34 安全

1. 在軟體開發生命週期（SDLC）的設計階段，必須先進行結構化的評估，以在編寫程式碼之前識別和解決潛在的安全風險、漏洞和架構缺陷（「安全設計審查」），並採取符合 OWASP 等行業標準的預防性和檢測性控管措施。
2. 必須強制執行安全編碼做法。

3. 供應商必須將資安控管整合至其應用程式、產品及服務的選擇、開發及實施流程及程序中。
4. 供應商應具備安全組建程序，供所有儲存、處理和/或傳輸 Citi 資訊之所有系統使用，並必須具備所有系統之安全圖片或範本。

17.35 惡意軟體防範控管

供應商應確保實施控管措施以預防並偵測任何惡意程式碼之入侵（例如，病毒、蠕蟲、木馬病毒、廣告軟體、間諜軟體、勒索軟體，或其他可損及資料的類似網路攻擊）。供應商必須：

1. 在所有個人電腦上實施、更新和維護防毒及防間諜軟體的技術，以及在所有區域網路（LAN）伺服器、郵件伺服器及其他儲存、處理及/或傳輸 Citi 資料的裝置上實施、更新和維護防毒技術。
2. 部署安全設定以防止終端使用者停用防毒/反惡意軟體工具及預定的安全掃描。
3. 具有可配置及更新防毒和反惡意軟體的中央管理自動化程序。
4. 確保實施可識別及處理不合規電腦（電腦上的防毒簽章或掃描引擎已過期）的流程。
5. 控制對通訊埠/介面之存取，以允許連線至外部裝置，包括但不限於儲存媒體。

17.36 行動程式碼控管

供應商應確保針對安全行動程式碼實踐執行控管措施。在授權使用行動程式碼之情況下，相關配置應至少符合所有相關的產業標準及應向 Citi 承擔的合約義務，且供應商應確保該授權之行動程式碼乃根據明確定義且明文規定之安全政策操作，同時防止執行未經授權之行動程式碼。

對於會影響基礎作業系統或平台之行動程式碼（例如，於「沙箱」以外），供應商應確保以下事項：

1. 供應商發佈之行動程式碼應由 Citi 認可之認證機構簽名認證，且證書之適用週期應由供應商管理以處理此證書的過期或換新事項。
2. 已簽署但證書已過期之行動程式碼應自正式上線環境中移除。

17.37 稽核記錄

供應商應確保所有用以存取、儲存、處理、管理和/或傳輸 Citi 資料之所有管制資訊系統，都在基礎設施或應用程式層級維護稽核追蹤記錄，以記錄下列項目：

1. 相關平台基礎設施安全之相關行動
2. 所有與防火牆或 IDS/IPS 產生之安全事件相關聯的系統警報
3. 所有未遂之系統安全違規情況（例如，使用者登入嘗試失敗）
4. 未經授權而企圖存取資源（軟體、資料、流程等）
5. 管理員行動
6. 與使用者或另一系統所接收的特定資訊有關的資訊
7. 所有有關財務交易及 Citi 資訊之重大事件，具體包括以下項目：

- a. 金融交易更新
 - b. 機密級或敏感 PII 級資料更新
 - c. 限制性資料更新
 - d. 身份認證資料更新
8. 已建立的所有工作階段
9. 為了支援詐欺調查且技術上可行，應取得工作階段工件，例如唯一的裝置 ID，並登入 Citi 相關應用程式（即，網站及行動應用程式）。這些工件必須至少包含 IP 位址。必須取得此類工件，以用於 Citi 交易及 Citi 開戶活動。必須取得這些資訊，使工作階段記錄可以連接至交易或開戶活動。
10. 稽核追蹤應記錄活動的負責人士，以防止其否認。
11. 必須記錄重大的資安管理（ISA）事件，具體包括以下項目：
 - a) 建立使用者
 - b) 修改使用者存取權
 - c) 在管制資訊系統上刪除設定檔，或建立、修改設定檔
 - d) 重設密碼
 - e) 系統安全配置變更
 - f) 特權功能 ID 的所有互動式活動
 - g) 除非技術上不可行，否則安全性記錄文件應包括至少以下資訊，無論系統產生何種日誌：
 - I. 事件發生日期及時間（UTC 時間格式）
 - II. 執行此動作之個人的使用者 ID
 - III. 事件類型
 - IV. 受影響之資產或資源名稱
 - V. 存取類型（刪除、修改等）
 - VI. 事件成功或失敗
 - VII. 來源（終端、端口、位置、IP、主機名稱等）

17.38 日誌資訊之保護

供應商應確保實施存取控制，以保存稽核追蹤在儲存和傳輸時的啟動、關閉操作過程中的完整性。

1. 為防止擅自修改稽核日誌，供應商應確保日誌不被系統使用者覆寫或修改；日誌原本就在追蹤系統使用者的活動。
2. 供應商應向 Citi 提供日誌資料之記錄保留流程，該流程定義資料之維護方式，並包括參考所有適用法律及法規要求的合規措施。
3. 組織或安全域內所有相關資訊處理系統之時鐘，應與準確的時間源同步。

17.39 使用監視系統

供應商應確保直接採集、記錄並審核以下事件，或透過自動審查流程執行這些步驟；這些事件包括：

1. 所有與防火牆或入侵偵測系統（IDS）/入侵防禦系統（IPS）產生的安全事件相關聯的系統警報。
2. 對於如安全標準版本中所識別為重要資源之所有更新。

3. 由任何身份（功能性、特權、系統、臨時身份等）執行的所有互動式活動，且可存取被分類為機密 PII 或更高層級的資訊。
4. 上述稽核記錄章節所列出的重大 ISA 活動，以下除外：
 - a) 對於透過端對端完整性控管之自動化工作流程/履行系統執行資安管理活動的使用者、職務或設定檔移除權限。

17.40 日誌關聯性與審查

1. 如果記載於日誌中的事件觸發警示，便將檢視此事件。如果顯示已出現可能會造成損害的資安事件時，供應商應展開後續追蹤行動及調查。
2. 供應商應確保將稽核日誌彙整至一個中央日誌管理系統中，例如安全資訊和事件管理（SIEM）系統或可進行日誌關聯性分析及審查的日誌分析工具中。
3. 供應商應定期檢視和調整其 SIEM 或日誌分析工具的配置，以改善對可行動事件的識別。

17.41 操作軟體控管

供應商必須確保只使用目前被業界接受之商業提供者所支援的作業系統及軟體，或具有有效及適當發佈修補程式及配置更新以解決安全問題者。

供應商必須確保實施明文規定之流程，具體指出已執行所有核准的安全修補程式及配置的修補期間。

無論供應商和 Citi 之間是否另有任何維護協議，供應商都應確保為 Citi 開發並受授權協議管理下的軟體不得用已知有漏洞且沒有支援的軟體版本，並確保此類軟體是按規定及時更新和修補。

用來處理 Citi 資訊的應用程式軟體必須向知名供應商購買，且必須取得授權、登錄記載和得到支援服務。

17.42 漏洞和威脅管理

1. 供應商應實施漏洞和威脅管理流程，以全面解決及/或包括以下所有項目：
 - a. 發現和管理所有處理、儲存、存取、傳輸 Citi 機密資料或更敏感資料資產中的漏洞的工具及流程。
 - b. 要求至少每週使用產業公認的漏洞工具與報告方法進行掃描。
 - c. 根據最新版本的「常見漏洞評分系統」（CVSS）作出漏洞排名（請參閱 <https://www.first.org/cvss>），並且根據嚴重性提供修復時間表。
 - d. 要求在進行全面正式上線部署之前，先測試漏洞修復。
 - e. 是一個記錄在案且可重複的操作流程，以加速修復關鍵漏洞。
 - f. 供應商必須在其整個可支援的生命週期中追蹤資產，以準備生命週期結束（EOL）或供應商支援結束（EOVS）的狀態，並設有主動升級或替換此類資產的流程。
 - g. 透過情報搜集、漏洞掃描或滲透測試發現的任何嚴重的 CVSS 評分漏洞，都必須在與漏洞風險相當的明確時間內優先處理和修復。

17.43 第三方託管的應用程式

如果供應商在網站或網際網路可存取的系統上，或 Citi 品牌的網站上具備或儲存 Citi 機密資料或更敏感的資料，則為了防止涉及可能會影響 Citi 的產品或服務的漏洞或威脅（每個都是一種「漏洞」），供應商必須遵守以下規定：

1. 任命一位供應商人員來回應 Citi 對於資安事項的查詢。
2. 每週至少一次利用產業認可的最佳做法查詢主要的電腦安全漏洞資訊專業機構的資訊，例如 FIRST、CERT/CC、CISA Known Exploited Vulnerabilities Catalog 等，以及廠商郵寄清單，並採取適當措施以取得相關服務包、修補程式、升級和解決方法、並且徹底測試、應用，最後再提供給 Citi。
3. 每季度至少一次使用網路、系統和應用程式等的漏洞掃描工具及/或滲透測試，來測試其資安措施的實施情況。
4. 允許 Citi 或 Citi 核准的第三方在合理的時間間隔內執行漏洞評估、道德駭客或其他安全評估，以確認供應商是否遵守任何合約和此處規定的義務，包括但不限於審查政策、流程和程序；實體安全措施的現場評估；網路、系統和應用程式漏洞掃描以及滲透測試，並且使用商用工具及/或產業標準做法來執行這些檢驗。
5. 任何將向供應商提供漏洞評估服務的承包商都必須是選自於 Citi 核准的漏洞評估提供者名單。如果供應商使用承包商或分包商執行此服務，則供應商必須自費確保本規定所要求的任何漏洞評估應如同供應商直接提供這些服務一樣及時完成，並應確保要求任何承包商或分包商促成完成任何此類評估的規定應記錄在供應商與承包商/分包商之間的服务協議中，包括授權 Citi 執行此類評估的文字。
6. 通知。
 - a) 如果供應商發現涉及影響 Citi 的產品或服務的漏洞，供應商將在發現後的 24 小時內以書面通知 Citi，並包括供應商正在採取的修復行動的說明。
 - b) 如果供應商根據其責任規定而在公開披露流程管道（在國家漏洞資料庫（NVD）中或透過提供給外部資安廠商的威脅目錄中發佈漏洞）後發現涉及影響 Citi 的產品或服務的漏洞時，供應商將在此類發佈後的 24 小時內以書面方式通知 Citi。每次通知都將包含有關此漏洞的資訊、系統對於與 Citi 有關服務的功能（即，系統是否託管 Citi 資訊或是否用於提供服務或兩者兼具）、是否可以遠端使用；以及常見漏洞與披露（CVE）分數。在漏洞被修復之前，供應商將繼續向 Citi 提供修復的最新情況。如果 Citi 發現漏洞，Citi 可能會就此向供應商發出通知，而供應商應根據本節的規定立即修復此漏洞。
7. 修復行動。對於在本節下所提供的每個漏洞通知，通知方將根據對 Citi 的嚴重性和風險評估此類漏洞的風險等級和影響，並根據附錄 A 中所載明的常見漏

洞評鑒系統（CVSS）指定一個風險優先順序等級（請參閱 <https://www.first.org/cvss>）。一旦指定了風險層級並由各方同意後，供應商將修復任何所發現的中級、高級或關鍵級漏洞。如果可能，對於任何此類漏洞的修復，都應能在目前所部署的發佈版本的安全包中提供。

如果供應商無法或不願將漏洞修復到 Citi 滿意的程度，Citi 可以終止適用的授權而不承擔任何進一步的責任或財務義務（對於終止的部分），而供應商應立即按比例將已支付的該部分的授權費退還給 Citi。

17.44 通訊安全網路控管

1. 用以存取、儲存、管理、處理和/或傳輸 Citi 資訊之供應商網路，應受保護以免受威脅，且必須使用此網路中的執行點維護資訊系統之安全性。
 - a. 分類為 Citi 機密或更高層資訊之資訊，不應一直儲存於系統網際網路之隔離區（DMZ）。用於存取、儲存、管理、處理及/或傳輸 Citi 資訊之網路若使用無線區域網路（WLAN）或其他包含合理控管以禁止未授權存取之無線裝置解決方案（PEAP-TLS、EAP-TTLS 等）可連接至含有 Citi 資訊的網路。
 - b. 所有連接至供應商全球網路之外部 IP 皆由供應商管理之防火牆的保護。
 - c. 具備即時入侵偵測系統（IDS）或入侵防禦系統（IPS），以監控和保護連結至可存取、管理、儲存、處理或傳輸 Citi 資訊之網路的網際網路連線。
2. 對於所有 Citi 品牌的網際網路應用程式，供應商必須確保：
 - a. 在供應商網站上託管的服務應有 Citi 核准之防分散式阻斷服務（Distributed Denial of Service, DDoS）的保護，或 Citi 驗證之類似控管機制。
 - b. 外部防火牆之配置必須使用「預設為拒絕」規則。防火牆規則之配置應基於最小權限原則，且被防火牆拒絕（例如丟包）的所有連線嘗試都應予以計入日誌/記錄。
 - c. 網路通訊流量應預設為拒絕，而應在託管介面中為例外允許的情況。這種例外情況必須僅限於特定來源、目的地及服務。
 - d. 網站應用程式流量應有適當的控管並過濾，例如使用網站應用程式防火牆。

17.45 網路分隔

供應商應確保用於存取、儲存、處理、管理和/或傳輸 Citi 資訊並可透過網際網路存取之所有資訊系統及應用程式僅可透過供應商的隔離區（DMZ）存取。

供應商在緊急事件中應能夠過濾網路區域磁碟分割之間的訪問權限，以降低網路安全事件之影響（例如病毒爆發期間的端口過濾）。

遠端存取及主機安全應執行以群組為基礎的存取控管（例如員工、分包商），以限制供應商網路中對網路資源之存取權。於主機層級，存取權限控管得以於群組或個人層級完成。

17.46 網路中的設備識別

技術平台必須辨識並且驗證與交互作用及其他緩解掌控的 IS 風險層級相當的同級技術平台。

1. 只有遵守這些規定並經供應商授權之供應商裝置（例如，硬體，包括但不限於桌上型電腦、筆記型電腦）可存取儲存、處理或傳輸 Citi 資訊所在之供應商網路。
2. 只有遵守本規定及經 Citi 授權之供應商裝置（例如，硬體，包括但不限於桌上型電腦、筆記型電腦、卸除式資料儲存媒體）才可存取 Citi 網路。

17.47 安全性規定分析及規格

供應商必須將資安程序整合至其應用程式、產品及服務的選擇、開發及實施流程及程序中。

17.48 線上交易

1. 如果適用時，供應商應備有使用動態密碼或數位憑證以驗證憑證之資訊系統。
2. 所有終端法人憑證必須至少每 13 個月更換一次。
3. 可儲存、處理、管理、存取 Citi 資訊，託管 Citi 品牌網際網路應用程式，或可連結至 Citi 網路資源等的供應商應用程式都必須：
 - a. 使用的驗證方式是根據所存取的資料類型/功能類型；
 - b. 實施多重要素驗證（MFA）合規評估並在需要時實施建議；
 - c. 實施可疑活動監控（SAM）上線評估並在需要時實施建議；
 - d. 所有這些情況供應商都應聯絡其主要業務聯絡人以瞭解 Citi 目前規定。

17.49 變更控管程序

1. 供應商應確保防火牆、入侵偵測系統（IDS）及入侵預防系統（IPS）之配置變更有經過供應商之變更管理流程。
2. 應記錄並監控透過臨時 ID 所授予之正式上線權限，以追蹤其對環境所為之變更。
3. 對於包含 Citi 分類為機密或更高層級，或資安風險組成中屬高「完整度」或高「可用性」的顧客資訊之管制資訊系統，供應商必須審閱依第 17.32 節（稽核記錄）規定取得之日誌。此審查得採用適當的風險抽樣方法完成。
4. 此審查應驗證屬於暫時特權存取權限之變更已如預期完成。
5. 供應商必須記錄所有變更，包括儲存審查過程的證據。

17.50 資訊洩露

供應商應具備明文規定的安全編碼標準，以防止資訊洩漏，內容包括：

1. 詳細的系統資訊（例如，伺服器類型及技術）。
2. 顯示樹狀目錄結構及基礎資料庫類型之堆疊追蹤及例外錯誤。

17.51 測試資料

供應商不得在軟體應用程式開發或測試環境或實驗室中使用或儲存 Citi 分類為機密或較高層級資訊，除非使用符合產業標準的工具和方法，對資訊進行去識別化、遮罩及/或模糊

處理，以便此類資料不再具敏感性，否則供應商必須在開發或測試環境中實施現場正式上線控管。

17.52 系統驗收

供應商應明文規定，符合相關產業規範之專案範圍管理及系統驗收流程。

17.53 資安弱點通報

供應商應具備相關流程，以確保於應用程式及基礎設施漏洞對 Citi 資訊資產有不利影響時，能立即通報 Citi。

17.54 安全事件責任和程序

1. SIRT 是一項安全事件，無論此安全事件如何發生、在哪發生，或誰可能造成此外洩都會損及：
 - Citi 資料的保密性、完整性或可用性。
 - Citi 必須遵守合約、法律或監管等義務的任何資料（包括個人資訊）的保密性、完整性或可用性。
 - 儲存、處理或傳輸任何 Citi 資訊的 Citi 資訊系統之完整性或可用性。
2. 為了我們的目的，保密性遭破壞是指資料外洩給未經授權的人，或 Citi 喪失保管及控管資料的情境。所有安全事件都必須立即報告。
3. 如果供應商遭遇了 SIRT，供應商必須與 Citi 合作，根據 Citi 自己的事件回應流程提供 Citi 要求的資訊、分析遭到外洩的資料以讓 Citi 能夠滿足法律、法規和/或內部治理要求；根據法律、法規或規章的要求，或 Citi 酌情決定是否需要，並由供應商承擔費用，在 Citi 有機會審查和修改建議的通知範本語言之後方可發出任何/所有通知；且供應商不得在任何此類通知中指出 Citi，除非 Citi 以書面特別要求指出 Citi。

17.55 資料外洩防護（DLP）

供應商應實施資料外洩防護（DLP）控管機制，包括涵蓋所有可存取 Citi 機密或更高層級資訊的人員之內容及端點監控。

供應商應設有控管機制，以偵測和/或防止 Citi 機密或更高層級資訊透過以下管道從其網絡中被移出的情形：

- a. 未加密電子郵件
- b. 加密電子郵件的附件
- c. 列印 Citi 資料
- d. 將 Citi 資料轉發至網絡外地點（例如透過 FTP）

- e. 企圖將 Citi 機密或更高層級資料複製到卸除式媒體，例如隨身碟、抽取式硬碟、CD/DVD 光碟及其他附有資料儲存功能的卸除式裝置。預設應避免此一權限。
- f. DLP 解決方案必須記錄所有事件並警示供應商；這些事件顯示要將 Citi 機密或更高層級資料從其網絡中移動、傳送或複製至其他目的地的企圖（無論是否成功或遭到封鎖）。預設應避免此高權限。
- g. 上傳 Citi 資料至外部網站，包括 SaaS/檔案共享網站。預設應避免此高權限。

17.56 網路瀏覽

1. 供應商應設有網路存取控管機制，以防止分享 Citi 機密或更高層級資訊，和防止可存取 Citi 資訊的員工曝露於惡意軟體或攻擊的風險中。
2. 可存取 Citi 機密或更高層級資訊的供應商：
 - a. 必須記錄所有網址請求。
 - b. 對於嘗試存取可用來未經授權分享 Citi 資訊的網站（即，網頁郵件、聊天、社群媒體、網上儲存空間、Gen-AI 等）進行封鎖。
 - c. 必須封鎖可讓環境曝露於惡意軟體或攻擊中的網站之存取權限。
 - d. 必須封鎖嘗試存取被視為與業務無關的網站。
 - e. 供應商應訂閱定期進行更新的網址分類服務；基於預設，所有未經分類的網址都應預設為封鎖對象；或所有網址都應預設為封鎖對象，再按個案分別核准。
 - f. 供應商使用中的網站瀏覽器應獲得全面支援，並具有軟體供應商提供的最新安全性更新。

17.57 電子訊息傳送

除非按照第 17.9 節（加密控管使用政策）所述對所有 Citi 資訊進行適當加密，否則不得使用即時通訊、點對點網路或其他網際網路協作工具傳輸或儲存 Citi 資訊至供應商網路外，或傳輸或儲存來自存有 Citi 資訊之網路。

17.58 電子郵件

供應商應設有電子郵件控管機制，以防止分享 Citi 資訊而曝露於惡意軟體或攻擊的風險中。這包括：

1. 掃描進入電子郵件匣道的傳入之檔案附件；如果可對系統構成風險則予以封鎖。
2. 使用最新版電子郵件過濾軟體（反垃圾郵件、反網路釣魚）。
3. 當任何 Citi 機密或更高層級資料傳送至供應商公司之外時都必須進行加密。
4. 供應商使用中的「電子郵件客戶」可獲得完整支援，並具有軟體供應商提供的最新的安全性更新。

17.59 卸除式媒體

1. 供應商必須保護 Citi 資訊，無論其儲存於何種媒體上。本標準適用但不限於以下存有資訊之媒體類型：卡片、卡式磁帶、光碟（CD）、庫存檢查表、磁碟

片或其他卸除式儲存裝置，硬拷貝輸出、磁碟、磁帶、縮影膠片、縮影單片、光碟或紙類文件。

2. 存有 Citi 資訊之系統的可攜式媒體/儲存裝置，其存取之預設設定必須為無存取權限。若因例外而授予讀寫權限時，則在可攜式媒體裝置上的資料必須加密。
3. 如果可使用卸除式媒體，則此類使用必須透過管理層核准步驟，包括需要使用卸除式媒體的業務原因。卸除式媒體必須由管理階層進行庫存清點。內含 Citi 機密或更高層級資訊的卸除式媒體必須自動加密，且使用者無需採取行動。

17.60 媒體處置

1. 分類為 Citi 機密或更高層資訊之 Citi 資訊，根據 Citi 提供之說明，已符合處置之資格時（例如，Citi 已不再需要或使用該資訊，且超過法律、法規和/或 Citi 政策所要求之任何額外保留期已經過期），則供應商必須銷毀該資訊，使其不可使用且不可復原。
2. 必須使用經過核准且可透過特定、不同的字元隨機覆寫硬碟磁區的工具，以根據以下規則安全地刪除可安裝媒體：
 - a. 對於儲存被分類為機密或更高層級資訊的媒體工具，必須完成媒體的三個通行流程。
 - b. 對媒體進行消磁（如適用）。
3. 實際銷毀媒體以讓它不可讀取（例如用碎紙機銷毀或壓碎硬碟）。
4. 包含機密或更高層級資訊的紙本及其他非電子儲存媒體在進行最後處置前，必須安全地予以收集並儲存於安全的「機密箱」中。機密箱必須隨時上鎖，且僅可由授權人員開啟。
 - a. 可能包含 Citi 機密或更高層級資訊的具有記憶/儲存功能的影印機、印表機、傳真機及任何其他裝置都必須加以清理。

17.61 資安管理和培訓

1. 保有一套適當的網路/資訊安全意識和教育計劃，包括但不限於預防網路釣魚和其他社會工程攻擊、妥善處理機密級或更高層級的資訊以及資安事件報告和回應管理。
2. 供應商應確保所有員工，包括承包商和臨時工作人員，都接受與其工作職能相關的組織政策和流程方面的適當意識教育和培訓。
3. 供應商應確保每年對此一培訓和意識計劃進行審查和更新，以處理網路安全環境中出現的風險和威脅、認識當前最佳做法和新技術。
4. 至少應包括以下主題：
 - b. 資訊標記與處理
 - c. 安全傳輸（安全電子郵件、安全的 SharePoint 儲存、勿將 Citi 擁有的資料傳送至個人電子郵件中）
 - d. 資安事故通報
 - e. 安全工作場所（例如，適當的網際網路使用方法、未經授權的軟體、禁止下載未經核准的軟體）
 - f. 密碼管理（例如：強密碼、禁止密碼分享）
 - g. 社交工程（例如：網路釣魚、魚叉式網路釣魚、簡訊網路釣魚）
 - h. 遠端工作（例如：防護/安全連線、個人裝置安全性）
5. 供應商員工必須在獲得託管 Citi 資料的系統存取權限時或之前被指派接受培訓，並在指派通知中的截止日期前完成培訓。
 - a. 在法律允許的情況下，應每年至少對所有人員進行一次資安事件培訓。
6. 在當地法律允許下，培訓應包含可記錄有效性評估（例如，完成培訓後要接受有通過/失敗門檻的測驗）的工件。

17.62 網路風險管理計劃

供應商還應至少具備一份適當的網路風險管理計劃，且至少包括以下各項：

1. 持續運行一套明確定義、記錄在案的資安風險管理計劃，及/或具有明確定義的網路/資訊風險管理部分的營運風險管理計劃；該計劃定義供應商的網路風險胃納，並確保其網路殘餘風險與該胃納保持一致。
2. 持續運行一套堅實的安全風險管理治理計劃，包括但不限於，收集及/或執行旨在評估組織內整體安全狀態的安全稽核及審查結果，並定期每年至少一次向高階主管報告，以審查並確保供應商並未違反其網路風險胃納。
3. 持續遵守適用於供應商處理、儲存及/或傳輸信用卡/扣帳卡交易、付款及/或資訊的任何 PCI 資料安全性標準（PCI-DSS）。
4. 持續運行一套符合產業標準的危機管理計劃和手冊以及安全事件回應團隊計劃，以確保供應商有足夠和充分的能力，能偵測、遏制、調查、回應任何未遂、疑似及/或實際的網路安全事件並能從中復原。

17.63 應用程式、API、代碼、系統和基礎設施安全

如果供應商管理、開發、共同開發、提供開發環境及/或提供軟體應用程式，供應商應對所述軟體的軟體及/或軟體修補程式執行代碼審查，以找出安全漏洞、防止未經授權的存取和修改，及/或惡意軟體或其他形式的惡意代碼的植入，以及漏洞測試，以確保應用程式（包括 API）和相關系統服務、操作系統和網路，免於發生任何已知的漏洞和缺陷，這些皆可導致資安事件、隱私洩露、詐欺、未經授權的存取及/或機密資訊的披露，該應用程式所處理、儲存或傳輸的資訊喪失完整性，及/或可影響供應商提供給 Citi 的產品和/或服務品質的可用性損失。

17.64 行動安全性

若供應商提供行動應用程式解決方案，則此供應商應遵守以下規定：

1. 行動應用程式必須僅支援 Google Android（不包括 Android Go）和/或 Apple iOS/iPadOS 平台的一般可用（GA）、穩定和非 EOL² 版本。如果行動解決方案已配備支援其他作業系統/版本，則所支援的作業系統/版本應由 Citi 進行配置。
2. 行動解決方案不應支援未配備常規指示組以支援加密演算法之行動平台/裝置，包括但不限於本文件第 17.9 節（加密要求）中所規定的加密。
3. 未正式發佈的操作系統版本，包括但不限於 Beta 版、搶先試用版和功能預覽版/發行版，在正式環境中不允許使用。
4. 供應商必須能夠提供整合後的第三方組成部分的清單，包括但不限於由行動解決方案組合/使用的免費且開放來源的軟體庫。
5. 行動應用程式必須遵守可使其透過 Apple App Store 或 Google Play Store 等公共應用程式商店發佈的規定和最佳做法。所列出的公共應用程式商店應為散播/發佈行動應用程式的首選主要方法。
6. Android 行動應用程式必須使用 APK 簽章配置（第 2 版本以上）。不得使用 APK 簽章配置版本 1（也稱為 JAR 簽章）。
7. 行動應用程式簽章金鑰類型和時間長度必須遵守本文件的 17.9 節- 加密要求所述。
8. 每個應用程式簽名金鑰和相關的 X.509v3 憑證都必須個別管理，並專用於單一的應用程式 ID/套件組合 ID。簽章金鑰不得在應用程式之間共用。
9. 如果行動應用程式要求保留行動裝置上的資料，則應用程式必須僅保留裝置上的應用程式/服務目的所需的最新資料，或法律/監管規定所要求的資料。
 - a. 使用者資料的收集、處理和/或儲存必須符合當地法律，包括但不限於隱私法規，例如一般資料保護條例（GDPR）和 2002/58/EC（電子通訊隱私，即 ePrivacy）指令或其地區同等規定。
 - b. 整合的第三方組成部分（例如資料庫）不得收集、處理使用者資料和/或儲存使用者資料。

² 由平台擁有者或供應商持續提供支援，並定期接收安全性與維護更新的产品版本。

10. 行動應用程式不得讓任何應用程式資料全局存取。
 - a. 如果需要與其他應用程式分享資料，則這些應用程式必須利用商業上合理的技術、方法、控管措施，讓個別作業系統僅將必要的資料數量與少數其他應用程式分享，且此類資料分享的理由充分並被記錄下來。
11. 行動應用程式必須僅使用個別行動作業系統提供的安全通訊設施。例如：
 - a. **Android** 應用程式必須在其應用程式中明確聲明，不允許不安全的網路流量流向其資訊清單及/或網路配置檔案中的任何網路網域。
 - b. **iOS/iPadOS** 應用程式都必須一律開啟應用程式傳輸安全（ATS）功能，無任何例外情況。
12. 加密材料應繫結至硬體支援的安全金鑰儲存庫（keystore）中。
13. 行動應用程式必須以發佈模式內建且不得包含：
 - a. 任何可跳過安全控管措施的功能或方法，
 - b. 除錯資訊，是指可促成逆向工程的資訊，例如原始碼檔案名稱、變數名稱、符號名稱、評論等。
14. 行動應用程式必須具備有效的防釣魚或防篡改機制，以防止注入可在運行過程中改變或監控應用程式行為的惡意代碼。
15. 行動應用程式必須實施全面防除錯或防逆向工程/代碼混淆技術，以防止逆向工程攻擊。
16. 行動應用程式套件必須具備可驗證其內容之真實性及完整性（例如，使用加密總和檢查碼及/或數位簽章）的能力。
17. 如果行動應用程式需要使用者身份驗證，則應在使用者身份驗證開始之前完成應用程式及/或裝置的完整性檢查。
18. 凡是存取/處理/儲存任何屬於 Citi 且分類為 Citi 機密或更高層級，以及/或其 IS 風險分類為「中級」或更高層級資訊的行動應用程式必須僅使用強大的生物識別模式（例如，符合或超過相應的 [Android Compatibility Definition Document](#) 中定義的 Class 3 / Strong 類別）。
19. 行動應用程式必須實施防範措施，以防範中間人（MitM）攻擊。
20. 行動應用程式必須能夠偵測遭到入侵的裝置，包括但不限於「被破解」或「被刷機」的行動裝置，並根據企業的風險評估及監管要求做出回應。
21. 行動應用程式必須實施強大的裝置繫結，以防止軟體權杖（例如，攔截證明）遭到複製。
22. 行動應用程式必須使用安全的鍵盤應用程式/解決方案（例如，由行動作業系統內建/預先安裝的應用程式）。
23. 推送通知不得包含任何敏感資訊（例如，被分類為機密或更高層級的 Citi 資訊）。但是，可透過推送通知發送一次性密碼（OTP）。
24. 行動應用程式解決方案必須具備拒絕/取消與使用已知漏洞/可攻擊漏洞的應用程式版本之行動客戶進行通訊嘗試的能力。
25. 行動應用程式必須遵守產業最佳實踐方法，包括但不限於 [OWASP Mobile Top 10](#) 中發佈的防範技術。

26. 利用人工智慧和機器學習（AI/ML）技術的行動應用程式必須符合道德規範，並根據第 19 節-人工智慧/機器學習（包括生成式 AI/代理型AI）
27. 行動應用程式必須僅使用執行 Citi 所需目的/功能的最低裝置權限。
28. 行動應用程式不得將任何非公開資訊儲存在外部/卸除式儲存裝置中，例如 SD 卡。

17.65 軟體披露事項

供應商應披露任何和所有軟體組件，包括但不限於提供給 Citi 的產品或服務中所內含的開放原始碼軟體（統稱為「軟體組件」）。供應商不得在事先未向 Citi 披露的情況下透過更新、升級或以其他方式將任何軟體組件納入任何將安裝在 Citi 系統的產品或服務版本中。此外，供應商應確保其產品或服務不包括會使 Citi 或其附屬公司承擔 Citi 在協議中未明確披露和接受的任何義務而授權的任何軟體組件。供應商應向 Citi 披露在供應商組織、產品或服務內發現的任何惡意軟體組件，並且在發現後的 30 天內通知 Citi。具體而言，供應商應向 Citi 提供 OWASP CycloneDX 檔案格式或 ISO/IEC 5962:2021 軟體組合資料交換（SPDX）規格檔案格式的軟體物料清單（SBOM），以披露供應商在產品或服務的每個發行或每個版本中使用軟體組件的情況。此類披露必須包括此軟體組件的來源（例如，企業廠商、嵌入式資料庫、公共二進位套件管理器、從原始碼建置的軟體，或任何嵌入式軟體，或精選軟體組件供應商），以及此供應商或其任何軟體供應鏈依賴項是否複製了此軟體組件（稱為「分支」），且隨後是否將其建立在產品或服務中作為套件依賴項，或作為整合至供應商原始碼中的原始碼，以供匯編產品與服務之用。

17.66 威脅模型分析

供應商應實施威脅模型分析流程，以全面解決及/或包括以下所有項目：

1. 範圍定義：供應商必須清楚定義威脅模型範圍，專注於處理、儲存或傳輸 Citi 機密級與更高層級資訊的軟體組件及資料流。
2. 威脅識別：供應商必須在設計生命週期早期考量各種攻擊向量及威脅主體，以系統性識別與此軟體的設計、架構及預期用途相關的潛在威脅及漏洞。
3. 風險分析：供應商必須分析已發現的威脅以評估其潛在影響和可能性，以優先處理安全風險。
4. 控管整合：供應商必須定義適當的安全控管機制及緩解策略，並將其整合至軟體的設計及開發中，以處理這些需優先處理的風險。
5. 文件記錄：供應商必須記錄威脅模型，包括已發現的威脅、相關風險以及已實施的相應緩解措施。
6. 定期審查：供應商應定期審查並更新威脅模型，特別是軟體的設計、功能或配置環境有重大改變時。

17.67 人工智慧

1. 供應商應實施並遵守提供給 Citi 或與 Citi 整合的所有 AI/ML 系統及組件的安全軟體開發生命週期（SSDLC）。其中包括安全設計、開發、測試、配置和持續維護。
2. 供應商提供的 AI 系統應證明營運中的完整性，並展現對於對抗性攻擊的強大抵抗能力。其中包括實施提示詞注入偵測、輸入淨化和維持資料隔離等機制。
3. 供應商提供的 AI 代理及組件應與 Citi 的系統及其他工具進行互動。這需要強大的身份和存取權管理、對於工具執行參數進行嚴格驗證以及隔離高風險工具的操作。必須納入人機迴圈（HITL）機制，以應對敏感或高風險的行動。
4. 供應商 AI 系統必須為所有重大事件生成全面、不可變更的日誌，且可進行稽核。這些日誌必須有免於被篡改及彙整的保護，且將根據 Citi 政策進行保存。同時必須具備持續監控及異常偵測能力，以識別與安全相關的事件及可疑活動並提出警示。
5. 供應商的 AI 系統必須支援以風險為基礎的人力監督，允許適當的介入，並在設計時明確界定 AI 輸出與行為的責任歸屬。其中包括按風險等級對 AI 輸出進行分類，並支援人力覆寫能力。
6. 供應商提供的所有 AI 代理、組件、系統等都應實施強大的身份和存取管理控管。每個 AI 互動都必須歸因於身份識別（人力或非人力），且所有存取權限都需要驗證。AI 代理在存取 Citi 資源時應使用託管身份並遵守最低特權原則。
 - a. 供應商應提供並確保所有 AI 代理都被指定為 Citi 目標識別網絡（COIN）代理身份，且與 Citi 的身份和存取管理（IAM）系統一致，以便實施 Citi 安全政策、集中身份管理和稽核。
 - b. 供應商應使用 Citi 核准的整合機制，包括透過安全閘道（例如 SSG Gateway 或 Apigee）提供的 COIN API，讓第三方代理商加入 COIN 並應確保此類加入是根據 Citi 適用的安全要求以安全方式進行。
 - c. 供應商如果是內部託管，則應生成與 COIN 一致的權杖；外部託管的供應商，如果使用自己的聯合權杖進行入站身份驗證，則需要有受支援的 Citi 權杖兌換權杖，例如，從 MSFT 兌換為 COIN 權杖。凡是目前未透過此交換支援的新權杖類型都必須接受審查，以取得 Citi 的 IAM 團隊核准。
7. 若供應商使用或提供 Model Scention Protocol（MCP）伺服器或客戶端，則供應商必須實施 MCP RFC 7591，包括所有可選功能。
8. 供應商 AI 系統應保護系統提示及內部運作機制免於外洩或惡意操縱。情境管理必須實施嚴格的界限，以防止租戶、使用者或環境之間的資料外洩。
9. 對於特定 AI 的安全事件，供應商應記錄此事件的偵測、回應和報告等程序，包括涉及 AI 系統的對抗性攻擊、模式操縱、未經授權的 AI 行動或資料外洩。任何此類事件都必須立即通知 Citi。

18 安全工作場所指導方針

適用於可存取/處理/儲存/管理/儲存 Citi 資訊及/或託管 Citi 品牌網際網路應用程式及/或可連結至 Citi 的網路資源及/或必須在無需陪同下自行進入 Citi 設施的供應商。

供應商必須保護 Citi 及其客戶的有形及無形資產。Citi 及客戶資產僅得以經核准的方式（例如，按照適用的許可證、條款與條件使用）用於經核准的用途，且僅得與 Citi 和 Citi 供應商之業務目的相關。資產包括現金、證券、實物財產、服務、經營計劃、Citi 資訊、供應商資訊、分銷商資訊、智慧財產權（電腦程式、模型及其他物品）及所有其他個人、專有和機密資訊。侵佔 Citi 資產或擅自披露 Citi 資產違反您對 Citi 負有之責任，並可能構成對 Citi 的詐欺。同樣，浪費 Citi 資產、疏於照護 Citi 資產或擅自使用 Citi 資產也違反您對 Citi 負有之責任。

項目	規定
Citi 資訊（電子及影印文件）	供應商於正常工作時間結束後以及任何時間在離開指定工作場所時都應將 Citi 資訊鎖好以維護資訊安全。
桌上型個人電腦（PC）和筆記型電腦	用於存取或檢視任何 Citi 資訊之 PC 及筆記型電腦，如果閒置一段時間後應使用螢幕保護程式密碼鎖住。每當供應商離開指定工作場所時必須以 CTRL+ALT+DEL，再選擇「Lock Computer」（鎖住電腦）以鎖住 PC 和/或筆記型電腦。若供應商使用筆記型電腦查看 Citi 資訊，供應商應確保在上班時間中要使用底座之電腦線纜鎖或安全鎖保護筆記型電腦，並於下班後鎖好。
鎖住	存放 Citi 資訊的檔案櫃及抽屜皆應在下班時鎖住。
開放式辦公區域	開放式辦公區不得用作儲存 Citi 資訊的檔案伺服器/迷你資料中心，除非此空間是專為此用途設計且 Citi 已記錄在案。
印表機、影印機及傳真托盤	印表機、影印機及傳真托盤皆不得有 Citi 相關的文件留下來。
處置方式	對於不再需要（保留特定時間後）的 Citi 資訊要妥為處置。文件應以碎紙機碎掉，或置於安全/上鎖的回收箱中。遵循適當之刪除程式後，應安全處置磁性媒體。

19 人工智慧/機器人學習（包括生成式 AI/代理型 AI）

適用於使用人工智慧/機器學習（AI/ML）的供應商，包括生成式 AI/ 代理 AI，如 Citi 在此《供應商規定》中對於他們所提供的產品/服務的任何部分中所定義。

19.1 供應商不得使用並確保任何分包商未使用以下所述之 AI/ML，除非雙方已根據合約之適用時間表或工作單中同意此類使用：

- a. 被使用、包含或以其他方式納入供應商根據合約直接或間接向 Citi 提供的任何產品或服務或任何部分中，包括其中所含或內置的任何第三方產品或服務；或
2. 以任何方式在供應商履行任何合約時被使用（無論此類 AI/ML 是否被使用）、包含或以其他方式納入交付給 Citi 的實際產品或服務中；或
3. 被供應商以任何可能將 Citi 資訊曝露給此類 AI/ML 的方式使用，包括但不限於，被供應商在其非商業業務營運中使用的任何 AI/ML（例如，業務記錄保存、流程改進、研發、合規和內部稽核）。

19.2 供應商未能遵守這些義務將被視為重大違反本協議條款。

19.3 如果監管機構要求，對產品/服務有使用 AI/ML 的任何部分進行任何監管檢查或取證調查時，供應商必須協助 Citi 回應監管機構的要求，包括進行及/或協助進行必要的演算法稽核以瞭解包括 AI/ML 模型的演算法的實際運作情況。

19.4 供應商還必須遵守以下原則：

合法性：供應商 AI / ML 應遵守適用法律。

目的和比例原則：供應商不得將內容或 Citi 資訊與供應商或任何第三方資料合併。未經 Citi 書面同意，供應商不得使用內容或 Citi 資訊進行 AI/ML 培訓。供應商 AI/ML 不應使用內容或 Citi 資訊，除非為提供這些服務所需。

20 顧客投訴

20.1 投訴是一種口頭或書面溝通，可以口頭（當面或透過電話）或書面（透過郵件或電子通訊，例如電子郵件、聊天或社群媒體等）以表達顧客、非顧客、潛在顧客、Citi 客戶、潛在客戶或客戶的授權代表（以上統稱「顧客」）對於 Citi、Citi 員工、Citi 承包商或代表 Citi 行事的第三方服務供應商，對於 Citi 政策或上述任何組合所提供之 Citi 產品或服務的不滿。

20.2 供應商必須遵守 Citi 顧客投訴處理政策，以及任何適用的 Citi 投訴相關標準和程序。供應商應在收到任何顧客（或根據 Citi 投訴定義的非顧客或潛在顧客）或任何監管機構就供應商代表 Citi 提供的服務或與 Citi 相關的其他事項提出的任何書面或口頭不滿或疑慮（以下簡稱「投訴」）後二十四（24）小時內，以書面通知其 Citi 業務主要聯絡人（或其指定人）。除非 Citi 向供應商提供一個可追蹤投訴的「追蹤系統」，否則供應商還將開發、實施和維護一個能讓 Citi 合理滿意的此類系統，用以追蹤投訴並在 Citi 酌情要求時向 Citi 提供報告副本或系統存取權。追蹤系統將：

- a. 依照類型、收件日期和向 Citi 提供投訴通知的日期對投訴進行分類，
- b. 追蹤投訴的處理過程，直至得出結論/解決為止，以及

- c. 針對 Citi 的合理要求為所有其他事項配合協助。此追蹤系統的設計必須能讓供應商判斷他們是否收到針對某特定事項的大量投訴，以便供應商（在與 Citi 協商後）可以確定是否存在與供應商的業務或其提供的服務有關的系統性問題以及時糾正。

21 個人交易及投資政策

Citi 的個人交易及投資政策（PTIP）對於以下事項作出定義，包括允許和禁止的交易和投資活動、預先核准要求事項，以及對適用人士的經紀或交易帳戶的維護、披露和監控的要求項目。本政策載明促進遵守法律及法規的最低標準，以防止不當使用個人的職位或與 Citi 的關係，包括個人對 Citi 或第三方的 (1) 重大非公共資訊或內部資訊（統稱為「MNPI」）；或 (2) 客戶的證券、衍生性金融商品及大宗商品部位、交易及策略等資訊。

所有需要定期存取 MNPI 以執行其在 Citi 的工作職責且被指定為適用人員和/或 Citi 存取人員的供應商員工都必須遵守 PTIP 中的規定。供應商人員應遵守 ICRM 有關個人帳戶披露、個人交易活動預先核准和個人交易限制及提交定期結帳單等要求。

22 計費及發票開立標準

在 Citi 改善服務時間及強化控管措施方面，所有供應商皆應遵守 Citi 提交發票之首選方法，以及發票付款首選選項，詳情如下：

- 供應商將建立傳送給 Citi 的電子檔案，格式為 Citi 與此供應商通訊的方式，及/或使用 Citi iSupplier 工具輸入應填入的發票/帳單資料，以便後續以數位方式傳輸給 Citi。
- 供應商將向 Citi 提供所有必要的銀行資訊及證明文件，以便於以電子方式付款給供應商及/或使用 Citi 提供虛擬卡付款（如適用）。

附註：付款條款從 Citi 收到提交的發票日期開始計算。

為及時付款並履行合約規定，Citi 要求所有供應商皆提供以下發票資料，並在向 Citi 開立貨物或服務帳單時遵守相關的指導準則：

1. 正確的 Citi 業務單位、「付款方」地址以及相關的 Citi 業務聯絡人姓名。
2. 發票號碼、發票日期及採購訂單號碼。
3. 發票應發送至 Citi 訂單詳情中的 Citi 地點或的電子郵件地址。
4. 帳單中的商品或服務必須在發票中有清楚且詳細的資料。

5. 僅包括此發票的本期款項（不包括其他待處理發票的未付餘額）。
6. 發票應以英文書寫，並包括證明文件。

23 強制離開職務政策

Citi 的 強制離開職務政策 要求執行敏感或高風險活動的人士，特別是影響公司帳本和記錄的人士應定期停止執行這些職責。這項強制執行的政策旨在透過創造機會來偵測可能仍然隱藏的潛在詐欺、盜竊或其他不當行為，以加強內部控管。本政策符合美國聯邦儲備委員會針對敏感職位人員需要離開工作崗的監督要求。

所有可存取敏感資料且其在 Citi 的工作職責且被指定為「敏感」人員的供應商員工都必須遵守 **Mandatory Absence** 政策的規定。敏感人士必須每年按照所有政策規定和限制來安排「強制性離開工作崗位期」並如實完成。在這段期間內，他們不得執行、指示、授權或核准任何敏感活動，也不應對任何通訊作出實質回應（包括客戶互動），但將查詢引導至他處則除外。如果在此段期間開始後需要中斷，主管或 Citi 業務聯絡人必須在合規系統中取消此離崗期，才能恢復系統存取權，之後此位員工必須重新安排新的離崗期。

附錄-定義

實體隔離是一種讓電腦、系統或網路在實體上與其他電腦、系統或網路隔離的安全性措施。使用實體隔離的資料備用架構可限制曝露於網路攻擊的風險，同時可讓資料恢復至攻擊開始之前的某個時間點。

適用法律包括：(a) 州止贖法律和法規，以及 (b) 多個美國聯邦機構公佈的規則、指導方針和其他相關規定，包括實施 2003 年《公平準確信貸交易法》（**Fair and Accurate Credit Transactions Act**）第 114 條的貨幣監理局（有時稱為紅旗警訊指導方針和法規）。

可用區域是指雲端服務提供者擁有的一組邏輯資料中心的所在地。可用區域是在雲端區域中的一個或多個離散資料中心，備有冗餘電力、網路連線和電信功能。

人工智慧（AI）是指一種定量方式、系統或方法（即「技術」），透過電腦程式模擬人類智慧，以超越傳統的統計、數學、計量經濟學或金融方法的方式做出評估、預測、建議或決策。其中包括以下載明的所有 AI 類別，以及各種不同的 AI 版本，例如：生成式 AI、代理型 AI、大語言模式、通用 AI（GPAI）模式等。

人工智慧類別包括：

- **靜態人工智慧**：是指離線以手動方式訓練出，或其參數是經過明確程式設計出的 AI 技術，用於做出評估、預測、建議或決策。
- **動態人工智慧**：是指有別於「靜態 AI」的技術，可以在正式上線環境中定期自動重新訓練參數。
- **自動人工智慧**：是指能夠額外自動變更其基本結構（例如，超參數、輸入變數）的「動態 AI」技術。
- **認知人工智慧**：是指可以自主做出決定並採取相應行動的技術，即使是對於沒有經過專門訓練去從事的事情。

機器學習（ML）是 AI 的子集，從資料中導出表述或推理，而無需對每個參數的表述或計算步驟進行明確的程式設計，例如隨機森林、神經網絡方法。相較之下，不屬於 ML 子集中的人工智慧技術，包括諸如模糊邏輯、用於自然語言處理的複雜依存句法技術。

業務活動負責人（BAO）是指 Citi 員工，負責執行和主動管理與供應商往來關係有關聯的某些活動。

業務介紹人是 Citi 聘請代表 Citi 採取行動以發掘新的業務機會或管理現有客戶關係的供應商。

商務禮品是 Citi 員工因 Citi 或外部機構業務，所提供或收受之（除商務招待外）任何有價之物，通常不包括 25 美元或以下之物品。

Citi 資訊是指 Citi 擁有或有義務在儲存、處理、傳送，或處置過程中以數位或非數位方式保護的資訊。

Citi 資訊分類包括：

機密性是指關於 Citi 業務及/或相關方的資訊，這些資訊不涉及個人且需要高度保護。此類

資訊的機密性、完整性或可用性遭到破壞可能會對 Citi 的營運、財務狀況、特許經營或企業客戶造成嚴重影響。

機密性個人身份識別資訊是指可能促成非法活動的某位個人的個人資訊，例如對此個人進行身份盜竊、信用詐欺或其他金融詐欺。此類資訊的機密性、完整性或可用性遭到破壞可能會對此個人造成重大影響，包括但不限於財務損失或詐欺。

- 與其他個人資料組合而構成機密性 PII 的個人資料元素包括個人姓名或聯絡資訊（地址、電話或電子郵件地址）結合了：
 - 可能導致資金流動或可用來進行身份盜用或詐欺的交易資料元素，例如：
 - 信用卡/扣帳卡號碼
 - 信用卡驗證值（CVV）或 PIN 碼
 - 信用報告資料（信用分數）
 - 完整的出生日期
 - 員工表現（評估/意見回饋），或薪酬資訊
 - 視訊錄影，包括 CCTV 及 ATM 記錄。
- 單獨的某些個人資料元素應構成機密 PII：
 - 美國社會安全號碼、政府核發的身份證號碼（在用途和/或受保護的合法地位上相當於美國社會安全號碼）、護照號碼、駕照號碼、個人的稅務 ID 號碼

內部資訊是供商業目的使用的非關個人資訊，需要中等層級的保護。此資訊的機密性、完整性或可用性遭到破壞可能會對團隊或工作團隊造成**有限的影響**。

- **個人身份識別資訊（PII）**是指以下的任何資訊：
 - 可識別或可用來識別個人或家庭（例如姓名、簽名、地址、社會安全號碼或居民註冊號碼等唯一的國家識別碼、出生日期、駕照號碼）。
 - 可關係到、描述、可被關聯到，或可合理被連結到（直接或間接）個人或家庭。
 - 可用來驗證個人身份或提供帳戶的存取權限（例如，
 - 使用者戶稱、電子郵件地址、密碼、PIN、身份證號碼、安全提示問題的答案）；或可關係到個人而且屬敏感性質者（例如個人醫療或健康資訊、帳戶號碼、帳戶價值。）
 - 個人資料也包括受保護的健康資訊（如美國《健康保險可攜性及責任法案》（Health Insurance Portability and Accountability Act）所定義）、敏感性個人資訊及信用資訊（如各種資料保護/隱私權及銀行保密法所定義）。

公開資訊，即可在 Citi 之外自由獲取之資訊，或用於公共目的之資訊，例如 Citi 新聞稿或於 Citi 相關新聞中出現的文章。

限制性資訊是指對於 Citi

或其附屬公司是最具敏感性而限制於特定人士或團體使用的資訊，需要最高層級的保護。此資訊的機密性、完整性或可用性遭到破壞可能會對 Citi 的營運、財務狀況、特許經營或企業客戶造成**嚴重（整個公司、多個地區、多個部門）影響**。

- **敏感 PII 資訊**是指被特定法律指出需要額外保護的個人資訊，

有可能被用來非法歧視個人，或以其他方式對個人造成不公平或傷害。資訊的機密性、完整性或可用性遭到破壞時可能會對個人造成重大影響（包括但不限於財務損失、詐欺或歧視性影響）。

- 特別與以下資訊相關的資料：種族、宗教、宗教或哲學信仰、人種、政治立場或觀點、工會會籍、犯罪背景資訊或刑事犯罪、基因資料、生物識別資料或關於個人的性取向或性活動的資料。

- 個人健康資訊（PHI），包括有關個人醫療病史或身心狀況的資訊。

客戶應指 Citi 之任何客戶或顧客，可能包括個人（例如自然人）及企業、機構、組織及法人實體。

雲端區域是雲端服務提供者集群資料中心的實際位置。

通訊設備、系統及服務是指在傳送書面、語音或電子通訊時使用的任何硬體、軟體或應用程式。電子商務頻道包括但不限於：電腦、筆電、平板電腦、行動裝置或手機，包括「自攜電子裝置」（BYOD）、黑莓手機、電話、傳真機（傳真服務）、內部網路及網際網路存取、Wi-Fi 服務、電子郵件服務、即時通訊服務，例如 Microsoft Lync、Skype 和 Bloomberg 訊息、具有嵌入式通訊功能的網站和應用程式、視訊會議或協作平台（例如 Zoom 或 Microsoft Teams）以及社群媒體服務、互動式資訊共享服務、第三方聊天室、電子公告板和部落格。

內容是指 Citi 的機密資訊和任何其他資料、報告、統計數字或任何類型的 (a) 由 Citi 或代表 Citi 或其附屬公司或由其客戶或代表其客戶、顧客或服務提供者直接或間接提供或供應給供應商的資訊，(b) 透過本服務所建立、產生的資訊，或 (c) 源自任何上述而來的資訊。

合約為一種由雙方或多方簽署之書面法律文件，其中包括要約、同意、斟酌、當事方的義務，以及目的之合法性。合約範例可包括產品及服務之主協議、工作說明書/工作指令、Citi 實體及供應商簽署之修正、附錄、時程表、訂單或任何其他書面文件。根據這些標準，保密協議（NDA）亦視為合約。

拒絕進入（DOA）測試驗證 Citi 業務流程所需供應商的人員配置及支援，能夠在指定之 RTO 內復原。

拒絕服務（Denial of Service, DOS）測試確認供應商的應用程式及支援 Citi 業務的主要基礎設施組成部分可在指定的 RTO 內復原。

「**儲放材料**」是指以下(i)-(vi) 小節所列內容的統稱，並視情況適用於在 Citi 環境內運行的 Citi 授權軟體或供應商為 Citi 提供的託管服務所使用的材料：

- (i) 用於開發、操作、維護和支援與 Citi 簽訂的協議中載明的授權軟體或託管服務軟體原始碼的同一複製版本（以及此類軟體或託管服務的所有後續版本），以及此類軟體的所有文件記錄（無論 Citi 是否已經擁有此類原始碼部分的副本）（即「**原始碼儲放**」）；
- (ii) 供應商對於授權軟體或託管服務的開發、操作、維護和支援方面擁有權利的任何第三方軟體的原始碼；
- (iii) 所有軟體工具的授權副本，例如需要將儲放材料中的原始碼轉換為可執行格式的偵錯工具、組譯器及編譯器等，以對此軟體或託管服務進行操作、維護和支援；
- (iv) 對於上述未提供的項目，則提供以下各項的任何文件：(A) 儲放材料的概況說明和操作；(B) 架構和基本程式功能；(C) 資料流資訊；(D) 詳細的記憶圖和列表；(E) 輸入/輸出端口

- 圖；(F) 允許具有適用程式語言的普通技能的程式設計師使用及修改包括在儲放材料中的原始碼的其他詳情；
- (v) 與此軟體或託管服務相關且合理所需的所有其他技術資訊，以便使 Citi 或代表 Citi 的合格的第三方能夠使用、操作、修改和加強軟體或託管服務；以及
 - (vi) 與此軟體或託管服務相關的所有使用的第三方軟體和技術的列表，包括有關在軟體中使用情況的合理詳細資料，以及此類軟體或技術提供者的聯絡資訊。Citi 確認並同意，此儲放材料不包含第三方的任何原始碼，但第 (ii) 節所載明者除外；以及
 - (vii) 關於託管服務：
 - a. 雲端託管的正式環境或特定雲端相關材料特定環境的縮小版複製品，以及複製 Citi 的正式上線環境所需的其他資訊，包括（但不限於）：諸如代碼、terraform 腳本、雲端資源、雲端形成範本、配置檔案、雲端租戶、雲端訂閱、docker 鏡像、基板圖像等基礎設施及基礎設施為軟體的源代碼；以及
 - b. 儲存在該軟體中的 Citi 資料副本。

電子通訊是透過電子方式、傳輸電纜或無線訊號由供應商人員發送、接收或使用的文字訊息或資訊。電子通訊包括但不限於簡訊、電子郵件、點對點訊息或即時訊息、部落格貼文、社群媒體貼文、透過簡訊應用程式（例如 WhatsApp、WeChat、Line、Signal 或 Viber）發送的訊息，並包括附件、螢幕截圖、錄製的語音或視訊檔案、即時語音或視訊，以及透過電子通訊設備、系統和服務所建立、接收、下載、儲存、傳輸、刪除或使用的檔案。

功能 ID 屬通用 ID，例如 ADMIN 或 ROOT，由個人或流程使用以存取安全系統。身份和存取管理（IAM）運作中的一項關鍵做法，是確保 Citi 擁有特定、明確的控制措施以防範使用功能 ID 時之風險。

特許經營關鍵流程/特許經營關鍵應用程式（FCA）是指這些經 Citi 確認攸關其成功執行特許經營關鍵業務職能的流程/應用程式。

詐欺是指專為欺騙他人的一種刻意的行為、不實陳述或遺漏，結果造成受害人遭受損失或加害人取得利益。

託管服務包括任何已安裝的應用程式，以及供應商所管理或使用以提供託管服務的任何設施和環境、所有應用程式和其他軟體、資料庫、網站、伺服器、硬體、網路、電信和其他設備，以及在託管服務環境中安裝或使用的其他技術，以及在每種情況下的所有更新和支援服務，但不包括所有內容和 Citi 的系統。

身份驗證資料（IVD）定義為安全問題（SQ）或知識基礎驗證（KBA）問題。安全性問題通常由應用程式定義並由最終使用者回答。例如母親的婚前姓氏、出生地點、最喜歡的冰淇淋等。這兩種類型的問題都必須視為驗證資料。

資安或「IS」是指電腦或電腦系統可免於遭到擅自存取或攻擊的受保護狀態，由於此一狀態，(a) 該電腦或電腦系統可持續使用及操作；(b) 電腦或電腦系統之完整性得以維持，以及 (c) 透過電腦或電腦系統儲存、處理或傳輸的資訊之完整性及機密性得以維持。

資安威脅是指在電腦或電腦系統上或透過電腦或電腦系統所進行的行為或活動（無論為已知或可疑），可能危害或不利影響其或另一個電腦或電腦系統之資訊安全。

資安漏洞是指在電腦或電腦系統中，可被一個或多個資安事件威脅所利用的任何漏洞。

非 Citi 客戶/非生成的收入定義為與生成收入活動無關聯的重要業務活動，包括法律、管理、法規和業務連續性等活動。

保密協議（NDA）乃是 Citi 與供應商之間的協議，其中資訊的交換、使用和披露皆受協議條款之規範。

開放原始碼軟體是指原始碼或編譯的電腦程式，且這些原始碼可供一般大眾使用或修改其原始設計。

人員：是指（無論是直接陳述或從內容中衍生），供應商及其附屬公司、董事、高級主管、員工、代理商、稽核員、顧問、服務提供者及承包商（不包括 Citi 人員）。供應商人員也包括任何分包商之董事、高級主管、員工、代理商、稽核員、顧問或其他代表。」

記錄資料庫是包含 Citi 記錄之類型、位置、日期等資訊之詳細列表，業務部門應於資訊留存期中恰當管理這些記錄。

資訊保留是對於記錄及資訊進行暫停修訂或銷毀的要求，直到發出該保留令的主管機關解除此項要求為止。

復原能力是指供應商產品及服務之交付體積、數量或速度，以產品及服務正常交付時之百分比顯示。

復原持續時間即供應商在復原模式中可持續營運之最大持續時間，以日曆天為單位。

復原點目標是指以小時為單位，說明過去業務中斷後，資料應復原之時間點。這是因重大事件導致 IT 服務可能遺失資料的最長目標期間。**RPO** 僅是在衡量發生會影響 IT 服務的重大事件時，可能遺失資料的最長時間期限。它並不衡量可能遺失多少資料。例如，截至前一天為止之處理內容。

復原時間目標為自服務中斷至復原提供產品及服務之間之持續小時數。

「**釋出事件**」是指以下任何一項或多項：

- (i) 供應商 (A) 無力償還或承認無力償還到期債務；(B) 進入任何國內或國外破產法或無力償債法律程序，且在七（7）個工作天內未完全中止訴訟程序，或在提交申請後四十五（45）天內未駁回或撤銷；(C) 為債權人的利益作出一般轉讓；或 (D) 由任何有管轄權的法院命令委任接收人、受託人、保管人或類似代理人接管或出售供應商大部分的財產或業務。

資源管理組織（RMO）專責 Citi 全球點對點資源管理，包括策略性供應源、採購到付款運作、人力辦公室和供應商管理架構。

RMO 採購經理是資源管理組織（RMO）內負責協商合約的商業條款、規定及定價的個人，包括 RFP 及其他供應商選擇活動、合約條款與條件之管理以及財務評估鑑定要求。

對個人帶來的**嚴重或災難性不利影響**，是表示該影響可合理對個人造成顯著不利影響，包括財務損失、失業或損失或難以就業、喪失人權、個人或公開羞辱或不當監禁。

分包商：分包商是第四方（個人或法人），是第三方聘僱來執行 Citi 發包給第三方的部分或全部服務或活動。

指導：

Q1：是否需要對所有第三方的分包商進行通報？

A1：只需要報告與正執行的服務相關的分包商。分包商執行的服務或活動的範例包括但不限於：

- * 執行科技或軟體服務以直接或間接支援 Citi 發包給第三方的服務或活動的分包商；或
- * 服務項目中包括可存取 Citi 機密或更高層級資訊的分包商；或
- * 與任何 Citi 現有或潛在客戶有直接或間接互動的分包商；或
- * 可在任何 Citi 營業場所內外無人陪同的情況下執行 Citi 文件的銷毀或封存服務的分包商；或
- * 支援核心銀行業務功能或服務（例如付款、收帳、放款等）的分包商。

供應商：在本「Citi 供應商規定」文件中，「供應商」一詞僅是指已簽訂業務安排而直接向 Citi 法人提供產品或服務的外來第三方，或支援 Citi 法人達成其業務目標者的外來第三方。外來第三方是指非 Citi 法人。供應商也可以是 Citi 法人的客戶或顧客，或可能支援與 Citi 客戶和客戶之間的互動；然而完全基於 Citi 的客戶或顧客所做的業務安排在本文件範圍中不被視為供應商關係。

暫時性資訊：一筆記錄是指 Citi 基於法律、監管或經核准的業務原因而有義務保留的最終、最完整的資訊版本。所有其他資訊都被歸類為「過渡性資訊」。