條款 I：「業務聯絡資訊」

若由「供應商」或 Kyndryl 之任一方處理他方之 BCI 者，則適用本「條款」。

1.1 不論 Kyndryl 與「供應商」於何處執行「供應商」之「服務」與「交付項目」交付有關業務，Kyndryl 與「供應商」均得處理他方之 BCI。

1.2 當事人之一方：

a) 不得基於其他目的而使用或揭露他方 BCI（明確說明如下：非經他方事前書面同意及受影響「資料當事人」所必要之事前書面同意，任一方當事人不得基於行銷目的而「出售」他方之 BCI 或使用或揭露他方 BCI）；及

b) 於他方提出書面要求時，應即刪除、修改、更正、歸還或提供他方 BCI 處理有關資訊、限制他方 BCI 之「處理」，或就他方 BCI 採取其他所合理要求之行動。

1.3 雙方當事人未就彼此之 BCI 訂立聯合「管控者」關係，「交易文件」之任何條款，均不得解釋為，亦不構成表示訂立聯合「管控者」關係之意圖。

1.4 Kyndryl 對 BCI 所為「處理」之其他詳細資料，請參閱「Kyndryl 隱私權聲明」(Kyndryl Privacy Statement)（網址：https://www.kyndryl.com/privacy）。

1.5 雙方當事人已實施技術及組織安全措施，未來亦持續維護，以防範他方 BCI 發生滅失、毀損、更改、意外或未經授權之存取及非法之「處理」等情事。

1.6 供應商發現涉及 Kyndryl BCI 的任何安全侵害後，應立即（在任何情況下不得晚於 48 小時）通知 Kyndryl。 供應商將提供此類通知至 cyber.incidents@kyndryl.com。「供應商」應提供 Kyndryl 所合理要求之前述安全侵害及「供應商」所為補救及還原行動之狀況等資訊。例如，合理要求之資訊可能包括就安全侵害或「供應商」所為補救及還原活動相關事項所作成之日誌，該等日誌應足以證明對「裝置、系統或應用程式」、「裝置、系統或應用程式」之鑑識影像，以及其他類似項目所為之特許存取、管理存取及其他存取。

1.7 若「供應商」僅「處理」Kyndryl BIC，且對任何其他資料或著作物或「Kyndryl 公司系統」不具存取權限，則該「處理」僅適用本條款及條款 X（「配合、查核及補救」）。

條款 II：「技術與組織措施 - 資料安全」

若「供應商」係「處理」Kyndryl BCI 以外之「Kyndryl 資料」，則適用本條款。「供應商」於提供所有「服務」與「「交付項目」時，均應遵循本條款之規定，俾以防範「Kyndryl 資料」發生滅失、毀損、更改、意外或未經授權之揭露、存取或其他非法之「處理」等情事。以下各項準用本條款之規定：「供應商」於其提供「交付項目」與「服務」時所操作或管理之所有 IT 應用程式、平台及基礎架構，包括所有開發、測試、代管、支援、作業及資料中心環境。

1. 資料之使用

1.1. 非經 Kyndryl 事前書面同意，「供應商」不得將其他任何資訊或資料，包括「個人資料」，加入或包含於「Kyndryl 資料」中，且「供應商」除基於提供「服務」與「交付項目」之目的外，不得基於其他目的而以彙整或其他形式使用「Kyndryl 資料」（例如：「供應商」不得為進行研究與開發，以建立新供應項目或產生「供應商」供應項目有關報告，而使用或重複使用「Kyndryl 資料」評估改善「供應商」供應項目之效率或方法）。除「交易文件」另有規定者外，「供應商」不得「出售」「Kyndryl 資料」。

1.2. 「供應商」不得將 Web 追蹤技術內嵌於「交付項目」，或將之納入「服務」之一部分（該等技術包括 HTML5、本端儲存體、第三人標籤或記號及網路信標 (web beacons)），但「交易文件」明文許可者不在此限。

2. 第三人之要求及保密

2.1. 「供應商」不得將「Kyndryl 資料」揭露予任何第三人，但經 Kyndryl 事前書面授權者不在此限。政府（包括主管機關）要求存取「Kyndryl 資料」者（例如：美國政府對「供應商」發出國家安全令，要求其取得「Kyndryl 資料」者），或依法必須揭露「Kyndryl 資料」者，「供應商」應以書面對 Kyndryl 為該要求或規定之通知，並給予 Kyndryl 適當機會對揭露進行救濟（法律禁止為通知者，「供應商」應透過法律行動或其他方法，採取其合理認定之妥適行動，俾就「Kyndryl 資料」之禁用與揭露予以救濟）。

2.2. 「供應商」對 Kyndryl 擔保下列事項：(a) 其員工中，僅限為提供「服務」或「交付項目」而須存取「Kyndryl 資料」之員工具有該存取權限，所為存取以為提供該等服務與「交付項目」所需者為限；及 (b)「供應商」已約束其員工遵循保密義務，規定其僅限依「條款」許可範圍使用及揭露「Kyndryl 資料」。

3. 「Kyndryl 資料」之歸還或刪除

3.1. 「供應商」應於「交易文件」終止或期滿時，或於 Kyndryl 所要求之更早期日時，依 Kyndryl 之選擇而刪除或歸還「Kyndryl 資料」。若 Kyndryl 要求刪除，「供應商」應依「業界實作典範」使資料難以辨認且無法重新組合或重新建構，並向 Kyndryl 證實所為之刪除。若 Kyndryl 要求歸還「Kyndryl 資料」，「供應商」應於 Kyndryl 合理期限內，依 Kyndryl 合理書面指示歸還。

條款 III：「隱私權」

若「供應商」係「處理」「Kyndryl 個人資料」，則適用本條款。

1. 處理

1.1 Kyndryl 指定「供應商」僅限基於提供「交付項目」與「服務」之目的，且依 Kyndryl 書面指示（包括「條款」、「交易文件」及雙方當事人所訂關聯基本合約所載指示），對「 Kyndryl 個人資料」進行「處理」而為「處理者」。若「供應商」未遵循指示者，Kyndryl 為書面通知後得終止「服務」中受影響之部分。若「供應商」認為前揭指示違反資料保護法者，「供應商」應立即於法定時限內通知 Kyndryl。

1.2 「供應商」應遵循「服務」與「交付項目」所適用之一切資料保護法。

1.3 「交易文件」之「附件」或「交易文件」本身，就「Kyndryl 資料」規定下列項目：

(a) 「資料當事人」之種類；

(b) 「Kyndryl 個人資料」之類型；

(c) 資料操作及「處理」活動；

(d) 「處理」之期間與頻率；及

(e) 「再處理者」清單。

2. 技術與組織措施

2.1 「供應商」將實施及維護條款 II（「技術與組織措施 - 資料安全」）及條款 VIII（「技術與組織措施 - 一般安全」）規定技術與組織措施，俾以確保達到其「服務」與「交付項目」所示風險所適用之安全等級。「供應商」確認並瞭解條款 II、本條款 III 及條款 VIII 之限制規定，並應遵循之。

3. 資料當事人之權利與要求

3.1 「資料當事人」要求履行有關「Kyndryl 個人資料」之「資料當事人」權利（例如：資料之更正、刪除及封鎖等權利），「供應商」應立即將該項要求告知 Kyndryl（應使 Kyndryl 及任何「其他管控者」有充分時間足以履行其法定義務）。「供應商」亦得立即指示「資料當事人」對 Kyndryl 為前項要求。「供應商」不得回應「資料當事人」所提出之要求，但屬法律規定或 Kyndryl 以書面指示其回應者不在此限。

3.2 倘若 Kyndryl 有義務將「Kyndryl 個人資料」相關資訊提供予「其他管控者」或第三人（例如：「資料當事人」或「主管機關」），「供應商」應提供資訊及採取 Kyndryl 所要求之其他合理行動，即提供一切資訊並採取 Kyndryl 所要求之適當行動，為 Kyndryl 提供協助，並應使 Kyndryl 得以及時回應「其他管控者」或第三人。

4. 再處理者

4.1 「供應商」於新增「再處理者」或擴充現有「再處理者」之「處理」範圍前，應事先對 Kyndryl 為書面通知，並於書面通知中指明「再處理者」之姓名及說明「處理」之新增或擴充之範圍。Kyndryl 得隨時基於合理理由對前揭新增「再處理者」或擴充範圍提出異議，有此情形者，雙方當事人應本誠實信用原則，共同處理 Kyndryl 之異議。Kyndryl 有權隨時提出前揭異議，若 Kyndryl 於「供應商」之書面通知日起 30 日內未提出異議者，「供應商」得委任新增「再處理者」或擴充現有「再處理者」之「處理」範圍。

4.2 「供應商」於「再處理者」對「Kyndryl 資料」進行「處理」前，應加以規定各獲准之「再處理者」必須遵循「條款」所定資料保護、安全及認證等義務。「供應商」對於各「再處理者」義務之履行，應對 Kyndryl 負完全責任。

5. 跨境資料處理

依下列規定使用：

所稱**「有適當保護層級國家或地區」**，指依適用資料保護法或主管機關決策認定為提供有關傳輸之適當資料保護層級之國家或地區。

所稱**「資料輸入者」**，指非設立於「有適當資料保護層級之國家或地區」之「處理者」或「再處理者」。

所稱**「歐盟定型化契約條款 (EU Standard Contractual Clauses, EU SCC)」**，指已施行選用條款（第 9 條第 (a) 款第 1 項與第 17 條第 2 項除外），並於 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en 正式公布之「歐盟定型化契約條款」（2021/914 委員會決策）。

所稱**「塞爾維亞定型化契約條款（「塞爾維亞 SCC」）」**，指由「塞爾維亞公眾利益與個人資料保護資訊委員會 (Serbian Commissioner for Information of Public Importance and Personal Data Protection)」採用，並於 https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx 公布之「塞爾維亞定型化契約條款」。

所稱「標準契約條款」("SCC")，指依適用資料保護法規定，就「個人資料」傳輸予非設立於「有適當資料保護層級之國家或地區」之「處理者」所必須簽訂之契約條款。

歐盟執委會標準契約條款之英國 (UK) 國際資料傳送附錄（亦稱「UK 附錄」），指的是已發布於下列網址的歐盟執委會標準契約條款之英國 (UK) 國際資料傳送附錄官方文件：https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/。

歐盟委員會定型化契約條款之瑞士附錄（瑞士附錄），係指歐盟執委會定期化契約之條款，依據瑞士資料保護主管機關（**FDPIC**) 之決定適用，符合瑞士聯邦資料保護法 (**FADP**)。

5.1 未經 Kyndryl 事前書面同意，「供應商」不得跨境傳輸或揭露（包括遠端存取）「Kyndryl 個人資料」。經 Kyndryl 同意者，雙方當事人應協力確保遵循適用之資料保護法。SCC 如係前揭法律規定之必要者，「供應商」於 Kyndryl 要求時應即簽訂 SCC。

5.2 EU SCC 有關規定：

(a) 「供應商」非設立於「有適當資料保護層級之國家或地區」者，「供應商」茲此以「資料輸入者」身分與 Kyndryl 簽訂 EU SCC，且「供應商」應依 EU SCC 第 9 條之規定，與各獲准「再處理者」簽訂書面合約，並應依要求提供 Kyndryl 合約副本。

(i) 除雙方當事人另有書面約定者外，不適用 EU SCC 之「模組 1」。

(ii) 若 Kyndryl 為「控制者」，則適用 EU SCC 之「模組 2」；若 Kyndryl 為「處理者」，則適用「模組 3」。依 EU SCC 第 13 條之規定，若適用「模組 2」或「模組 3」，則雙方當事人同意下列事項：(1) EU SCC 以主管監管機關所在歐盟成員國之法律為準據法；及 (2) EU SCC 所生任何爭議，悉由主管監管機關所在歐盟成員國之法院審理。若前揭第 (1) 項中之法律不允許第三方受益人之權利，則 EU SCC 以荷蘭之法律為其準據法，第 (2) 項項下因 EU SCC 所生任何爭議，悉由荷蘭阿姆斯特丹法院審理。

(b) 若「供應商」設立於「歐洲經濟區」，而 Kyndryl 為不受「2016/679 一般資料保護規章」拘束之「控制者」，則適用 EU SCC 之「模組 4」，且「供應商」茲此以資料輸出者之身分，與 Kyndryl 簽訂 EU SCC。若適用 EU SCC 之「模組 4」，則雙方當事人同意 EU SCC 以荷蘭之法律為其準據法，且因 EU SCC 所生任何爭議，悉由荷蘭阿姆斯特丹法院審理。

(c) 若「其他控制者」（如「客戶」或關係企業）依第 7 條中之對接條款 (docking clause) 要求成為 EU SCC 之當事人，則「供應商」茲此同意該項要求。

(d) 完成 EU SCC 之「附錄 II」所需之「技術與組織措施」，載明於前揭「條款」、「交易文件」本身及雙方當事人所訂關聯基本合約。

(e) EU SCC 與「條款」如有牴觸，優先適用 EU SCC。

5.3 UK SCC 有關規定：

(a) 「供應商」非設立於「有適當資料保護層級之國家或地區」者，應依下列規定：(i)「供應商」茲此以「資料輸入者」身分代表自己與 Kyndryl 簽訂 UK SCC；及 (ii)「供應商」應依 UK SCC 第 11 條之規定，與身為「資料輸入者」之各獲准「再處理者」簽訂書面合約，並應依要求提供 Kyndryl 合約副本。

(b) 「供應商」為設立於「有適當資料保護層級之國家或地區」者，「供應商」代表身為「資料輸入者」之各「再處理者」，與 Kyndryl 簽訂 UK SCC。「供應商」未能為前述「再處理者」簽訂 UK SCC 者，「供應商」應於允許該「再處理者」對「Kyndryl 個人資料」進行「處理」前，提供 Kyndryl 該「再處理者」完成簽署之 UK SCC，交由 Kyndryl 會簽。

(c) Kyndryl 與「供應商」所訂 UK SCC，應視事實所需，依 UK SCC 第 11 條之規定，作為「管制者」與「處理者」所訂 UK SCC，或作為「資料輸入者」與「再處理者」所訂連續書面合約。UK SCC 與「條款」如有牴觸，優先適用 UK SCC。

(d) 「其他管控者」，如「客戶」或關係企業，得要求成為其他「資料輸出者」。「供應商」茲此代表自己並代表其「再處理者」同意前揭要求。Kyndryl 應將其他「資料輸出者」告知「供應商」，進而「供應商」應將該等其他「資料輸出者」告知 其「再處理者」（身為該等其他「資料輸出者」之「資料輸入者」）。

5.4 關於「UK 附錄」：

a) 若供應商未設立於適用之國家或地區：(i) 該供應商則依據「UK 附錄」以 Kyndryl 進口商身分，受到上述歐盟 SCC 條款之約束（須視處理活動的環境而定）；(ii) 該供應商將與獲准之每一個再處理者簽署書面合約，並於 Kyndryl 要求時提供各份合約之副本。

b) 若供應商設立於適用之國家或地區，而 Kyndryl 是不受英國一般資料保護規章之約束（已納入歐盟（撤銷）條款 2018 年之英國 (UK) 法律）的控制者，則該供應商將依據「UK 附錄」以 Kyndryl 出口商身分，受到上述歐盟 SCC 5.2(b) 一節之約束。

c) 若其他控制者（如客戶或關係企業）要求成為 UK 附錄之合約方，則供應商因應允該類要求。

d) 「UK 附錄」中的附錄資訊（列於表三）可參見於適用的歐盟 SCC、這些條款、交易文件本身及關係方間相關聯的基本合約。 Kyndryl 或供應商於「UK 附錄」變更時，皆不得終止「UK 附錄」。

e) 若「UK 附錄」及這些條款存有任何歧異，將以「UK 附錄」為準。

5.5 「塞爾維亞 SCC」有關規定：

(a) 「供應商」非設立於「有適當資料保護層級之國家或地區」者，應依下列規定：(i)「供應商」茲此以「處理者」身分代表自己與 Kyndryl 簽訂「塞爾維亞 SCC」；及 (ii)「供應商」應依「塞爾維亞 SCC」第 8 條之規定，與各獲准「再處理者」簽訂書面合約，並應依要求提供 Kyndryl 合約副本。

(b) 「供應商」設立於「有適當資料保護層級之國家或地區」者，「供應商」代表設立於「無適當保護層級國家」之各「再處理者」，與 Kyndryl 簽訂「塞爾維亞 SCC」。「供應商」未能為前述「再處理者」簽訂「塞爾維亞 SCC」者，「供應商」應於允許該「再處理者」對「Kyndryl 個人資料」進行「處理」前，提供 Kyndryl 該「再處理者」完成簽署之「塞爾維亞 SCC」，交由 Kyndryl 會簽。

(c) Kyndryl 與「供應商」所訂「塞爾維亞 SCC」，應視事實所需，作為「控制者」與「處理者」所訂「塞爾維亞 SCC」，或作為「處理者」與「再處理者」所訂連續書面合約。「塞爾維亞 SCC」與「條款」如有牴觸，優先適用「塞爾維亞 SCC」。

(d) 基於規範將「個人資料」移轉至「無適當保護層級國家/地區」之目的，為完成「塞爾維亞 SCC」之「附錄 1」至「附錄 8」所需資訊，載明於前揭「條款」及「交易文件」之「附件」，或「交易文件」本身。

5.6 關於瑞士附錄：

(a) 根據第 5.1 節若發生 Kyndryl 個人資料轉移， 均受第 5.2 節的歐盟執委會定型化契約條款同意的瑞士聯邦資料保護法（FADP) 所約束， 並以依照以下修訂內容，採 GDPR 標準，約束瑞士的地區個人資料傳輸：

- 援引一般資料保護規定（GDPR），均應視為援引 FADP 同等條款；
- 瑞士聯邦資料保護及資訊委員會為主管機關，符合歐盟執委會定型化契約條款附件 IC 第十三條
- 若傳輸僅受受 FADP 約束，則瑞士法律為準據法；
- 歐盟執委會定型化契約條款第 18 條中的「成員國」，應擴展和包括瑞士，以允許瑞士資料主體在其常駐地區內行使權利。

(b) 為免存疑，上述主旨均非降低歐盟執委會定型化契約條款給予之資料保護，而僅將此保護層面擴展至瑞士資料主體。 若情況並非如此，則以歐盟執委會定型化契約條款為準。

6. 協助及記錄

6.1 「供應商」在考量「處理」性質之情形下，應採取適當技術與組織措施，協助 Kyndryl 履行「資料當事人」之要求與權利有關義務。「供應商」在考量其可獲取資訊之情形下，應協助 Kyndryl 確保遵循下述事項有關義務：「處理」之安全、「安全侵害」之通知與溝通及「資料保護影響評量」之建立，包括於必要時事先諮詢權責主管機關。

6.2 「供應商」對於各「再處理者」姓名與聯絡人詳細資料，包括各「再處理者」之代表與資料保護主管，應維持最新記錄。「供應商」應依要求提供 Kyndryl 前揭記錄，使 Kyndryl 得以及時回應「客戶」或其他第三人所提出之要求。

條款 IV：「技術與組織措施 - 程式碼安全」

「供應商」對「Kyndryl 原始碼」具有存取權限者，適用本條款。「供應商」應遵循本條款之規定，俾以防範「Kyndryl 原始碼」發生滅失、毀損、更改、意外或未經授權之揭露、存取及其他非法之「處理」等情事。以下各項適用本條款之規定：「供應商」於其提供「交付項目」與「服務」及「處置」「Kyndryl 技術」時所操作或管理之所有 IT 應用程式、平台及基礎架構，包括所有開發、測試、代管、支援、作業及資料中心環境。

1. 安全需求

依下列規定使用：

所稱**「受禁制國家/地區」**指有下列情形之國家/地區：(a)美國政府依 2019 年 5 月 15 日實施之「保護資訊及通訊技術與服務供應鏈安全行政命令」(Executive Order on Securing the Information and Communications Technology and Services Supply Chain) 載明為「外國對手」者；(b) 依「2019 美國國防授權法案」(U.S. National Defense Authorization Act of 2019) 第 1654 條列示者； 或 (c) 於「交易文件」中載明為「受禁制國家/地區」者。

1.1. 「供應商」不得為謀求第三人利益，而散布「Kyndryl 原始碼」或將之委由第三人保管。

1.2. 「供應商」不得允許將「Kyndryl 原始碼」放置於位在「受禁制國家/地區」之伺服器中。「供應商」不得允許位於「受禁制國家/地區」或造訪「受禁制國家/地區」（視造訪範圍而定）之任何人，包括其「人員」，基於任何理由而存取或使用「Kyndryl 原始碼」，不論「Kyndryl 原始碼」位於全球何處，且「供應商」不得允許於「受禁制國家/地區」進行需要前述存取或使用之開發、測試或其他工作。

1.3. 管轄區訂有必須對第三人揭露「原始碼」之法律或法律解釋者，「供應商」不得將「原始碼」放置或散布於該管轄區。「Kyndryl 原始碼」所在之管轄區，其法律變更或法律解釋可能致「供應商」須依規定對第三人揭露「Kyndryl 原始碼」者，「供應商」應即從該管轄區銷毀或移除「Kyndryl 原始碼」，該等變更後之法律或法律解釋於該管轄區仍具法定效力者，不得再將其他「Kyndryl 原始碼」放置於該管轄區。

1.4. 「供應商」不得直接間接採取行動，致使「供應商」、Kyndryl 或第三人承擔「2019 美國國防授權法案」(U.S . National Defense Authorization Act of 2019) 第 1654 條或 1655 條所規定之揭露義務。明確說明如下：除「交易文件」或雙方當事人所訂關聯基本合約明文許可者外，在任何情形下，非經 Kyndryl 事前書面同意，「供應商」不得將「Kyndryl 原始碼」揭露予第三人。

1.5. 若 Kyndryl 通知「供應商」下列情事之一，或第三人通知當事人之一方下列任一事項者：(a)「供應商」獲允許將「Kyndryl 原始碼」攜入以上第 1.3 節所規定之「受禁制國家/地區」或管轄區；(b)「供應商」已採用非「交易文件」或雙方當事人所訂關聯基本合約或其他合約許可之方式發行、存取或使用「Kyndryl 原始碼」；或 (c)「供應商」已違反以上第 1.4 節之規定；則在不限制 Kyndryl 依法或衡平法或依「交易文件」或雙方當事人所訂關聯基本合約或其他合約規定，處理前述未遵循法律情事之權利前提下，依下列規定：(i) 前述通知係對「供應商」所為者，「供應商」應立即與 Kyndryl 分享該通知；及 (ii)「供應商」應依 Kyndryl 之合理指示，於 Kyndryl 合理決定之時程（與「供應商」商議後定之）對相關事項為調查與補救。

1.6. 若 Kyndryl 合理認定「供應商」就「原始碼」所定政策、程序、管控或常規之變更，係處理網路安全、智慧財產竊取或類似或相關風險可能所必需者（包括在無前述變更之情形下，Kyndryl 於對若干「客戶」為銷售或於若干市場銷售時可能受有限制，或無法滿足「客戶」之安全或供應鏈需求等風險），Kyndryl 得聯絡「供應商」共同討論處理前述風險之必要行動，包括該等政策、程序、管控或常規之變更。於 Kyndryl 要求時，「供應商」應協同 Kyndryl 評估前揭變更之必要性，並施行雙方合意之適當變更。

條款 V：「安全開發」

若「供應商」擬將其本身或第三人之「原始碼」或「就地部署軟體」提供予 Kyndryl，或將「供應商」之「交付項目」或「服務」提供予「Kyndryl 客戶」，使其成為 Kyndryl 產品或服務，則適用本條款。

1. 安全備妥

「供應商」應配合 Kyndryl 據以評量相依於「供應商交付項目」之 Kyndryl 產品與服務安全備妥之內部程序，包括及時完整回應要求資訊（透過文件、其他記錄、相關「供應商人員」訪談等方式回應）。

2. 安全開發

2.1 本第 2 節僅適用於「供應商」擬將「就地部署軟體」提供予 Kyndryl 之情形。

2.2 「供應商」基於下列考量，業已實施並於「交易文件」期間，依照「業界實作典範」，持續實施網路、平台、系統、應用程式、裝置、實體基礎架構、事故因應及「人員」方面之必要安全政策、程序及控管：(a) 保護「供應商」或其所聘僱第三人所操作、管理、使用或基於或針對「交付項目」而以其他方式仰賴之開發、建置、測試及作業系統與環境；及 (b) 防範所有「交付項目」原始碼發生滅失、非法處置及遭受未獲權限之存取、揭露或更改等情事。

3. ISO 20243 認證

3.1 若將「供應商」之「交付項目」或「服務」提供予「Kyndryl 客戶」，使其成為 Kyndryl 產品或服務，則僅適用本第 3 節。

3.2 「供應商」應取得符合下列標準之認證：ISO 20243、「資訊」技術、Open Trusted Technology Provider、TM Standard (O-TTPS)、降低惡意污染與偽造產品（自主評量認證或依信譽良好獨立稽核員之評量所為之認證）。前述認證得以下列方式替代:「供應商」以書面提出要求，並經 Kyndryl 以書面核准者，「供應商」應取得符合同業等級標準之據以處理安全開發與供應鏈常規之認證（自主評量認證或依信譽良好獨立稽核員之評量所為之認證 - 需經 Kyndryl 核准）。

3.3 「供應商」應於「交易文件」生效日後 180 日內取得符合 ISO 20243 或同業等級標準之認證（經 Kyndryl 書面核准者），並於其後每隔 12 個月展延一次此認證（各次展延，均應依據當時最新版本適用標準（亦即 ISO 2024 或經 Kyndryl 書面核准之據以處理安全開發與供應鏈常規之同業等級標準為之）。

3.4 於 Kyndryl 要求時，「供應商」應即提供 Kyndryl 認證複本（所稱認證，指「供應商」依以上第 2.1 節與 2.2 節規定有義務取得者）。

4. 安全漏洞

依下列規定使用：

所稱**「錯誤更正」**，指更正「交付項目」中之錯誤或缺失之錯誤修正程式與修訂，包括「安全漏洞」。

「風險控管」，指已知可減少或避免「安全漏洞」風險之方法。

所稱**「安全漏洞」**，指「交付項目」在設計、編碼、開發、實作、測試、作業、支援、維護或管理上，處於可被人以未獲授權存取或惡意探索之方式攻擊之狀態，包括下列情事之一：(a) 存取、控制系統，或中斷系統之運作；(b) 存取、刪除、更改或擷取資料；或 (c) 變更使用者或管理者之身分、授權或權

限。「安全漏洞」，不論其是否被指定「一般漏洞披露 (CVE)」ID 或其他評分或正式分類，均可能存在。

4.1 「供應商」聲明並保證遵循下列規定：(a) 採用「業界標準實作典範」識別「安全漏洞」，包括透過持續動靜態原始碼應用程式安全掃描、開放程式碼安全掃描與系統漏洞掃描；及 (b) 遵循「條款」之規定，協助防範、偵測及更正「交付項目」及「供應商」從中據以建立及提供「服務」與「交付項目」之所有 IT 應用程式、平台及基礎架構中之「安全漏洞」。

4.2 「供應商」知悉「交付項目」或前揭 IT 應用程式、平台或基礎架構中之「安全漏洞」者，應依下表所定「嚴重性等級」與期限內，提供 Kyndryl「交付項目」所有版本版次之「錯誤更正」與「風險控管」：

嚴重性等級*
「緊急安全漏洞」為構成嚴重且可能影響全球之威脅。Kyndryl 得不論「CVSS 基本評分」而自行定義「緊急安全漏洞」。
「極嚴重」-「CVSS 基本評分」為 9 至 10.0 之「安全漏洞」。
「高度嚴重」-「CVSS 基本評分」為 7.0 至 8.9 之「安全漏洞」。
「中度嚴重」-「CVSS 基本評分」為 4.0 至 6.9 之「安全漏洞」。
「低度嚴重」-「CVSS 基本評分」為 0.0 至 3.9 之「安全漏洞」。

期限				
緊急	***極嚴重***	***高度嚴重***	***中度嚴重***	***低度嚴重***
4 日以內 - 由 Kyndryl Chief Information Security Office 定之	30 日內	30 日內	90 日內	依業界實作典範

*「安全漏洞」尚未評定「CVSS 基本評分」者，「供應商」應採用該漏洞性質與情況所適用之「嚴重性等級」。

4.3 「安全漏洞」已予公開揭露，且「供應商」尚未就該「安全漏洞」提供 Kyndryl「錯誤更正」或「風險控管」者，「供應商」應實施可能降低該漏洞風險且技術上可行之其他安全控管。

4.4 倘若 Kyndryl 不滿意「供應商」就前揭「交付項目」或應用程式、平台或基礎架構中之「安全漏洞」所為之回應，在不減損其他 Kyndryl 權利之前提下，「供應商」應立即安排由 Kyndryl 直接與負責「錯誤更正」交付事宜之「供應商」副總或同級高階主管討論疑慮之事項。

4.5 「安全漏洞」範例包括不再獲得安全修正程式之第三人程式碼或終止服務支援 (EOS) 開放原始碼。

條款 VI：「公司系統存取」

若「供應商」員工對「公司系統」具有存取權限，則適用本條款。

1. 一般條款

1.1 Kyndryl 將決定是否授權「供應商」員工存取「公司系統」。若 Kyndryl 為前揭授權，「供應商」應遵循本條款之規定，亦應使其具有前揭存取權限之員工遵循之。

1.2 Kyndryl 將指定「供應商」員工存取「公司系統」時得採用之方式，包括該等員工能否透過 Kyndryl 或「供應商」所提供之「裝置」存取「公司系統」。

1.3 「供應商」員工僅限為提供「服務」而存取「公司系統」，且僅限使用 Kyndryl 就該存取權限所授權之「裝置」。「供應商」不得針對「服務」或因「服務」而使用前揭 Kyndryl 所授權之「裝置」為其他自然人或法人提供服務，亦不得使用該等「裝置」存取「供應商」或第三人 IT 系統、網路、應用程式、網站、電子郵件工具、協同作業工具等等。

1.4 明確說明如下：「供應商」員工不得基於個人理由使用 Kyndryl 所授權之「裝置」存取「公司系統」（例如：「供應商」員工不得將個人檔案（如音樂、影像、圖片或其他類似檔案）儲存於該等「裝置」，亦不得基於個人理由從該等「裝置」使用網際網路）。

1.5 「供應商」員工，非經 Kyndryl 事前書面同意，不得複製可透過「公司系統」存取之「Kyndryl 著作物」（亦不得將「Kyndryl 著作物」複製至可攜式儲存裝置，如 USB 裝置、外接式硬碟或其他類似裝置）。

1.6 「供應商」應依要求，按員工姓名確認其員工於 Kyndryl 指定時段被授權存取且已存取之特定「公司系統」。

1.7 對「公司系統」具有存取權限之「供應商」員工，於其符合下列任一條件時，「供應商」應於二十四 (24) 小時內通知 Kyndryl：(a) 不再是受僱於「供應商」；或 (b) 不再需要進行該存取權限之工作。「供應商」應協同 Kyndryl 確認已立即撤銷該前員工或現行員工之存取權限。

1.8 「供應商」應即通報 Kyndryl 有實際發生或疑似之資安事件（如 Kyndryl 或「供應商」之「裝置」滅失，或「裝置」或資料、著作物或其他任何資訊遭受未獲權限之存取），並配合 Kyndryl 進行該等資安事件之調查。

1.9 非經 Kyndryl 事前書面同意，「供應商」不得允許代理商、獨立承包商或下包商員工存取「公司系統」；Kyndryl 同意前項存取者，「供應商」應視同該等人員為「供應商」員工，立約約束該等人員及其員工遵循本條款之規定，並應就各該人員或員工對於前述「公司系統」存取之一切作為與不作為，對 Kyndryl 負責。

2. 裝置軟體

2.1 「供應商」應指示其員工及時安裝 Kyndryl 所要求之所有「裝置」軟體，以利以安全方式存取「公司系統」。「供應商」或其員工均不得干擾軟體作業或軟體所啟用之安全特定功能。

2.2 「供應商」及其員工應遵循 Kyndryl 所規定之「裝置」配置規則，並於其他方面協同 Kyndryl 協助確保軟體之運作能符合 Kyndryl 之預期。例如，「供應商」不得置換軟體網站之封鎖或自動修補等特定功能。

2.3 「供應商」員工不得與他人共用其用於存取「公司系統」之「裝置」，或其「裝置」之使用者名稱、密碼等資訊。

2.4 若 Kyndryl 授權「供應商」員工使用「供應商裝置」存取「公司系統」，「供應商」應於經 Kyndryl 核准之「裝置」安裝及執行作業系統，並於 Kyndryl 指示後，於合理時間內升級至該作業系統之新版本或新作業系統。

3. 監督及配合

3.1 Kyndryl 具有無限制權利，得以任何方式，從任何位置，使用 Kyndryl 認為必要或適當之任何方法，在未事前通知「供應商」或其員工或他人之情形下，隨時監控及補救潛在入侵及其他網路安全威脅。前揭權利之範例如下：Kyndryl 得隨時行使下列行為：(a) 於「裝置」上執行安全測試；(b) 透過技術或其他方法進行監控、回復，以及檢閱通聯記錄（包括檢閱電子郵件帳號中之電子郵件）、儲存於「裝置」中或透過「公司系統」傳輸之記錄、檔案及其他項目；及 (c) 取得「裝置」之完整鑑識影像。Kyndryl 如需「供應商」配合履行其權利者，「供應商」應充分及時滿足 Kyndryl 就配合事宜所提出之要求（包括但不限於以安全方式配置「裝置」、於「裝置」上安裝監控軟體或其他軟體、分享系統層級連線詳細資料、於「裝置」上實施事故因應措施，以及提供「裝置」實體存取權限，以供 Kyndryl 取得完整鑑識影像或其他項目等要求，以及類似與相關之要求）。

3.2 Kyndryl 為保護 Kyndryl 而認為有必要撤銷任一「供應商」員工或所有「供應商」員工對「公司系統」之存取權限者，Kyndryl 得於未事前通知「供應商」或任一「供應商」員工或他人之情形下，撤銷該等存取權限。

3.3 Kyndryl 權利不受「交易文件」、雙方當事人所訂關聯基本合約或雙方當事人所訂其他合約之條款以任何方式妨礙、減損或限制之，包括可能規定資料、著作物或其他資訊僅限位於特定位置之條款，或可能規定僅限位於特定位置之人員才得以存取前述資料、著作物或其他資訊之條款。

4. Kyndryl 裝置

4.1 Kyndryl 具有所有「Kyndryl 裝置」之所有權，「供應商」則應承擔「裝置」危險負擔之風險，包括遭竊、蓄意破壞或過失所致滅失風險。非經 Kyndryl 事前書面同意，「供應商」不得更改「Kyndryl 裝置」或允許他人更改之，所稱更改，指對「裝置」所為任何變更，包括對「裝置」之軟體、應用程式、安全設計、安全配置或實體、機械或電子等設計所為之變更。

4.2 「供應商」應於無需使用「Kyndryl 裝置」提供「服務」後 5 個工作日內歸還所有「Kyndryl 裝置」，Kyndryl 提出要求者，「供應商」應遵循「產業實作典範」，同時銷毀該等「裝置」上之所有資料、著作物及其他資訊，不得保留任何複本，俾以永久消除該等一切資料、著作物及其他資訊。除合理之損耗外，「供應商」應自費以「Kyndryl 裝置」交付「供應商」時之相同狀況包裝「Kyndryl 裝置」，並將之歸還至 Kyndryl 指定之位置。「供應商」未遵循本第 4.2 節所定義務者，即構成「交易文件」及雙方當事人所訂關聯基本合約與任何相關合約之重大違約行為，所稱「關聯」，指對「公司系統」所為存取有利於進行各該合約項下「供應商」之作業或其他活動者。

4.3 Kyndryl 將為「Kyndryl 裝置」提供支援（包括「裝置」檢驗及預防性與補救性維護）。有維修服務需求時，「供應商」應即通知 Kyndryl。

4.4 軟體程式，為 Kyndryl 所擁有或 Kyndryl 有權為授權之行為者，Kyndryl 授與「供應商」暫時性權利，「供應商」得據以使用、儲存及製作足夠之複本，以支援其對「Kyndryl 裝置」之授權使用。「供應商」不得為下列行為：將程式傳輸予任何人、複製軟體授權資訊、或對程式為逆向組合、逆向編譯、還原工程或以其他方式解譯，但所適用之法律明示許可且不得以契約拋棄者，不在此限。

5. 更新項目

5.1 5.1 縱使「交易文件」或雙方當事人所訂關聯基本合約另有相反規定，Kyndryl 以書面通知「供應商」且無需取得「供應商」同意，Kyndryl 為解決適用法律或「客戶」義務之要求，對本條款為更新、補充或以其他方式修改本 VI 條款，俾以安全性實作典範或以 Kyndryl 為保護「公司系統」或 Kyndryl 認有必要採取之其他方式，因應任何推展。

條款 VII：「人員擴增」

符合下列情形者，適用本條款：「供應商」員工將所有工作時間投注於為 Kyndryl 提供「服務」且於 Kyndryl 場所、「客戶」場所或其家中執行該等服務，並僅限使用「Kyndryl 裝置」存取「公司系統」以提供「服務」。

1. 存取「公司系統」；Kyndryl 環境

1.1 「供應商」僅限使用 Kyndryl 所提供之「裝置」存取「公司系統」以提供「服務」。

1.2 「供應商」應遵循條款 VI（「公司系統存取」）對「公司系統」所為一切存取所定一切條款。

1.3 Kyndryl 所提供之「裝置」，為「供應商」及其員工僅限用於提供「服務」之唯一「裝置」，且僅限供「供應商」及其員工用於提供「服務」。明確說明如下：在任何情形下，「供應商」或其員工均不得使用其他裝置提供「服務」、不得為「供應商」之其他客戶而使用「Kyndryl 裝置」，且除了為 Kyndryl 提供「服務」外，亦不得基於其他目的而使用「Kyndryl 裝置」。

1.4 使用「Kyndryl 裝置」之「供應商」員工，得彼此共用「Kyndryl 著作物」及將該等著作物儲存於「Kyndryl 裝置」，惟該共用與儲存以順利執行「服務」所需為限。

1.5 除前揭於「Kyndryl 裝置」內所為儲存外，在任何情形下，「供應商」或其員工均不得從 Kyndryl 用於保存「Kyndryl 著作物」之 Kyndryl 儲藏庫、環境、工具或基礎架構中移除「Kyndryl 著作物」。

1.6 明確說明如下：非經 Kyndryl 事前書面同意，「供應商」及其員工未獲授權將「Kyndryl 著作物」移轉至「供應商」儲藏庫、環境、工具或基礎架構，或「供應商」之其他系統、平台、網路等等。

1.7 有下列情形者，條款 VIII（「技術與組織措施 - 一般安全」）不適用於「供應商」之「服務」：「供應商」員工將所有工作時間投注於為 Kyndryl 提供「服務」且於 Kyndryl 場所、「客戶」場所或其家中執行該等服務，並僅限使用「Kyndryl 裝置」存取「公司系統」以提供「服務」。在其他情形下，條款 VIII 則適用於「供應商」之「服務」。

條款 VIII：「技術與組織措施 - 一般安全」

若「供應商」提供 Kyndryl「服務」或「交付項目」，則適用本條款，但有下列情形者除外：「供應商」僅限於提供前述「服務」與「交付項目」時始對 Kyndryl BCI 具有存取權限（亦即，「供應商」將不「處理」其他「Kyndryl 資料」或對其他「Kyndryl 著作物」或「公司系統」不具有存取權限）、「供應商」之唯一「服務」與「交付項目」為將「就地部署軟體」提供予 Kyndryl，或「供應商」依條款 VII（包括其中之第 1.7 節）規定，以人員擴增模式提供其所有「服務」與「交付項目」者。

「供應商」應遵循本條款之規定，俾以防範下列情事：(a)「Kyndryl 著作物」發生滅失、毀損、更改、意外或未經授權之揭露或存取；(b) 非法「處理」「Kyndryl 資料」；及 (c) 非法「處置」「Kyndryl 技術」。以下各項適用本條款之規定：「供應商」於其提供「交付項目」與「服務」及「處置」「Kyndryl 技術」時所操作或管理之所有 IT 應用程式、平台及基礎架構，包括所有開發、測試、代管、支援、作業及資料中心環境。

1. 安全政策

1.1. 「供應商」將持續採用 IT 安全政策及常規，此等政策及常規係為「供應商」業務不可或缺之一部分，且為「供應商」所有「供應商人員」均須遵循之規定，並應符合「業界實作典範」。

1.2. 「供應商」對其 IT 安全政策與常規每年應至少審查一次，「供應商」為保護「Kyndryl 著作物」而認有必要修正此等安全政策與常規者，亦應予修正。

1.3. 「供應商」應持續採用適用於一切新聘僱人員之標準必要聘僱查核規定，並準用於所有「供應商人員」及「供應商」之全資子公司。前述規定，在當地法律許可之範圍內，應包括前科背景調查、身分查核證明及「供應商」認有必要進行之其他查核。「供應商」認有必要者，應定期重複實施及重新查核前揭規定。

1.4. 「供應商」每年均應對其員工實施安全與隱私權教育訓練，並要求所有員工每年均應證實其確實遵循「供應商」之行為規範或類似文件所訂定之「供應商」商業行為道德、機密性及安全政策。「供應商」對於具有「服務」、「交付項目」及「Kyndryl 著作物」元件管理存取權之人員，應予實施專為其「服務」、「交付項目」及「Kyndryl 著作物」職責與支援所為之其他政策與程序教育訓練，並於必要時維護所規定之法規遵循與認證。

1.5. 「供應商」應設計安全與隱私權措施，以保護並維持「Kyndryl 著作物」之可用性，包括透過「供應商」對所有「服務」與「交付項目」及對「Kyndryl 技術」所為一切「處置」所為之實作、維護、遵循需要安全與隱私權設計之政策與程序、安全工程及安全作業。

2. 資安事件

2.1. 「供應商」應依電腦資安事件處理「業界實作典範」，持續採用所規定之事故因應政策。

2.2. 「供應商」應調查「Kyndryl 著作物」是否遭受未獲權限之存取或使用，並應擬定及實施適當之因應計劃。

2.3. 供應商發現任何安全侵害後，應立即（在任何情況下不得晚於 48 小時）通知 Kyndryl。 供應商將提供此類通知至 cyber.incidents@kyndryl.com。「供應商」應提供 Kyndryl 所合理要求之前述安全侵害及「供應商」所為補救及還原行動之狀況等資訊。例如，合理要求之資訊可能包括就安全侵害或「供應商」所為補救及還原活動相關事項所作成之日誌，該等日誌應足以證明對「裝置、系統或應用程式」、「裝置、系統或應用程式」之鑑識影像，以及其他類似項目所為之特許存取、管理存取及其他存取。

2.4. 「供應商」應給予 Kyndryl 適當協助，俾能履行 Kyndryl、Kyndryl 關係企業及「客戶」就「安全侵害」應盡之法定義務（包括對「主管機關」或「資料當事人」為通知之義務）。

2.5. 非經 Kyndryl 以書面核准或依法令規定須為告知或通知者，「供應商」不得告知或通知第三人「安全侵害」直接或間接與 Kyndryl 或「Kyndryl 著作物」相關。「供應商」於其將法令規定通知散布予第三人前，該通知如直接或間接漏露 Kyndryl 身分者，應事前以書面通知 Kyndryl。

2.6. 「安全侵害」係因「供應商」違反「條款」所規定之義務所致者：

(a) 「供應商」所生費用，由「供應商」負擔，Kyndryl 對適用主管機關、其他政府及相關產業自治機構、媒體（依適用法律之規定）及「資料當事人」、「客戶」及他人為「安全侵害」通知，其所生費用亦由「供應商」負擔。

(b) 於 Kyndryl 要求時，「供應商」應自費設置電話客服中心，以回應「資料當事人」所提有關「安全侵害」及其所生後果之問題，且應持續營運電話客服中心，營運期間為自「資料當事人」人獲知「安全侵害」之日後一年之期間，或依適用資料保護法所定期間（以可提供較高保護效力者為準）。Kyndryl 與「供應商」應共同協力製作 Script 及其他著作物，供電話客服中心人員於回覆詢問時使用。或者，Kyndryl 對「供應商」為書面通知時，Kyndryl 亦得設置並持續營運其自己之電話客服中心，以取代要求「供應商」設置電話客服中心，「供應商」應賠償 Kyndryl 因設置及持續營運前項電話客服中心所生實際成本。

(c) 向選擇進行信用監管服務與信用回復服務登錄之「安全侵害」事件利害關係人為該事件之通知後，自通知日期起算一年之期間或適用資料保護法所定期間（以可提供較高保護力者為準），Kyndryl 因提供前述服務所生實際成本，由供應商給予賠償。

3. 「實體安全」與「門禁管制」（以下所稱「設施」，指「供應商」代管、處理或以其他方式存取「Kyndryl 著作物」之所在實體位置）。

3.1. 為防範「設施」遭受未獲授權之進入，「供應商」應設置適當之實體門禁管制設施，例如：屏障、卡控入口、監視器及人員接待櫃台。

3.2. 「供應商」應規定，須經授權許可，始得出入「設施」及其內之管制區（包括臨時出入），並應依工作職責與業務需求限制出入權限。「供應商」有核發臨時出入證者，其授權員工於訪客在「設施」及管制區時，應全程陪同。

3.3. 為適度限制「設施」內管制區之出入，「供應商」應實施人員出入之門禁管制，包括符合「業界實作典範」之多因子門禁管制，並應記載所有出入嘗試，記載事項應保留一年以上。

3.4. 有下列情形之一時，「供應商」應撤銷出入「設施」及其內管制區之權限：a) 授權「供應商」員工離職；或 b) 授權「供應商」員工已無有效業務需求而不必再出入。「供應商」應採用有正式記載事項之離職手續，包括立即將其從門禁管制名冊中除名，以及繳回實體出入識別證。

3.5. 「供應商」應採取預防措施，防範用於支援「服務」與「交付項目」及「Kyndryl 技術」之「處置」之所有實體基礎架構遭受天然或人為之環境威脅，例如：過高環境溫度、火災、水災、濕度、遭竊及蓄意破壞。

4. 存取、人為介入、傳輸及隔離控制

4.1. 「供應商」於其操作「服務」與「交付項目」及「Kyndryl 技術」之「處置」時所管理網路之安全架構，「供應商」對其所記載之相關資訊，應予保留。「供應商」應分別審查前揭網路架構，並應採取措施，以防範對系統、應用程式及網路裝置發生未獲授權之網路連線，俾以符合安全分區、隔離及防禦等深度標準。「供應商」不得使用無線技術代管及操作「代管服務」；但「供應商」得使用無線網路技術交付「服務」與「交付項目」及對「Kyndryl 技術」進行「處置」，惟「供應商」應予加密，並要求該等無線網路必須進行安全鑑別。

4.2. 「供應商」應持續進行各項措施，此等措施之設計，旨在以符合邏輯之方式隔開及防範「Kyndryl 著作物」曝露於未獲授權之人或遭其存取。此外，「供應商」對其正式作業環境、非正式作業環境及其他環境，應持續進行適當隔離，「Kyndryl 著作物」目前已存在於非正式作業環境或已傳輸至該環境者（例如：重製錯誤），「供應商」應確保該非正式作業環境中之安全及隱私權保護措施確實同於正式作業環境。

4.3. 「供應商」對傳輸中及處於靜止狀態之「Kyndryl 著作物」，均應予加密（但「供應商」對 Kyndryl 證明對處於靜止狀態之「Kyndryl 著作物」進行加密在技術上不可行，且 Kyndryl 對該項證明相當滿意者除外）。「供應商」對所有實體媒體（如有），例如：內含備份檔之媒體，亦應予加密。「供應商」應保留針對資料加密有關安全金鑰之產生、核發、散布、儲存、輪換、撤銷、回復、備份、銷毀、存取及使用所記載之各項程序。「供應商」應確保加密時所採用之特定加密方法，符合「業界實作典範」（例如：NIST SP 800-131a）之規定。

4.4. 若「供應商」需要存取「Kyndryl 著作物」，「供應商」所取得之該項「Kyndryl 著作物」存取權，應以為提供及支援「服務」與「交付項目」所需之最低限度存取權為限。「供應商」應規定，前述存取權，包括基礎元件管理存取權（亦即，特許存取權），應以個人、職責為依據，並應由授權「供應商」員工依權責劃分原則予以核准及定期查核。「供應商」應持續施行相關措施，確認並移除冗餘帳戶與靜止帳戶。「供應商」應於帳戶所有人離職，或於 Kyndryl 或授權「供應商」員工（例如：帳戶所有人之經理）提出要求後二十四小時內，撤銷具有特許存取權限之帳戶。

4.5. 為符合「業界實作典範」，「供應商」應持續採取相關技術措施，強制執行非作用中階段作業逾時、多次連續登入嘗試失敗後鎖定帳戶、高保護性密碼或通行詞組鑑別等措施，以及要求以安全方式傳輸及儲存該等密碼及通行詞組之措施。此外，「供應商」對於所有對「Kyndryl 著作物」所為之非主控台型特許存取，均應採用多因子鑑別。

4.6. 「供應商」應監控特許存取權之使用，並持續採取專為下列用途設計之安全資訊及事件管理措施：(a) 識別遭受未獲授權之存取與活動；(b) 協助針對前項存取與活動進行即時且適當之因應；及 (c) 啟用由「供應商」、Kyndryl（依「條款」中之查核權，以及「交易文件」或雙方當事人所訂關聯基本合約或其他相關合約本中之稽核權利為之）及他人所為之稽核，確認是否遵循所記載之「供應商」政策。

4.7. 「供應商」於日誌中依「業界實作典範」記錄所有用於提供「服務」或「交付項目」及對「Kyndryl 技術」進行「處置」之系統有關管理、使用者或其他存取或活動，日誌應予保留（於 Kyndryl 要求時並應出具日誌）。「供應商」應持續採取特定措施，用以防範該等日誌遭受未獲授權之存取、修改及意外或蓄意毀損。

4.8. 「供應商」對為其所有或由其管理，以及由其用於提供「服務」或「交付項目」或對「Kyndryl 技術」進行「處置」之系統，包括終端使用者系統，應持續採取運算防護措施，包括下列防護措施：端點防火牆、全磁碟加密、為處置惡意軟體與進階持續威脅所採用之簽章型與非簽章型端點偵測與回應技術、時間型螢幕鎖定，以及用以強制執行安全配置及修補要件之端點管理解決方案。此外，「供應商」亦應實施技術與作業控管，以確保僅允許已知且可信任終端使用者系統得使用「供應商」網路。

4.9. 為符合「業界實作典範」，「供應商」對從中呈現或處理「Kyndryl 著作物」之資料中心環境，應持續採取防護措施，包括入侵偵測與防範及阻斷服務攻擊之因應措施與風險管控。

5. 服務與系統完整性和可用度控管

5.1. 「供應商」應執行以下各項：(a) 每年至少執行一次安全與隱私權風險評估；(b) 於正式作業發布前，及其發行後每年，應就「服務」與「交付項目」及其對「Kyndryl 技術」所為「處置」執行安全測試與漏洞評量，包括自動系統與應用程式安全掃描及手動道德駭客入侵；(c) 商請合格獨立第三人每年至少依「業界實作典範」執行一次滲透測試，包括自動與手動測試；(d) 針對「服務」與「交付元件」各元件及就其對「Kyndryl 技術」所為「處置」執行自動化管理與例行查核，以確認其是否符合安全配置要件；及 (e) 依相關風險、不當運用及影響，補救已識別漏洞或未符合安全配置要件之部分。「供應商」於其測試、評估、掃描及執行補救活動時，應採取適當步驟，防止「服務」中斷。於 Kyndryl 要求時，「供應商」應對 Kyndryl 出具「供應商」當時最新滲透測試活動書面摘要，此報告至少應包括測試涵蓋供應項目之名稱、測試之範圍內系統或應用程式數量、測試日期、測試使用方法及發現項目高階摘要。

5.2. 「供應商」應持續執行專為管理有關將變更應用至其「服務」或「交付項目」或對「Kyndryl 技術」所為「處置」所致相關風險而設計之政策及程序。「供應商」於施行前揭變更前，包括受影響系統、網路及基礎元件等變更，應先於登錄變更要求中記載以下各項：(a) 變更之說明與原由；(b) 施行細節與時程；(c) 敘明對「服務」與「交付項目」、「服務」之客戶，或「Kyndryl 著作物」所生影響之風險說明書；(d) 預期成果；(e) 回復計劃；及 (f) 授權「供應商」員工之核准。

5.3. 「供應商」應留存其操作「服務」、提供「交付項目」及對「Kyndryl 技術」進行「處置」時所使用一切 IT 資產之清冊。「供應商」應持續監視及管理前揭 IT 資產、「服務」、「交付項

目」及「Kyndryl 技術」（包括該等資產、「服務」、「交付項目」及「Kyndryl 技術」之基礎元件）之性能（包括容量）與可用度。

5.4. 「供應商」應從符合「業界實作典範」之預先定義系統安全映像檔或安全基準線（例如：「網際網路安全中心」(Center for Internet Security, CIS) 評比）建置其於開發或操作「服務」與「交付項目」及對「Kyndryl 技術」進行「處置」時所使用之一切系統。

5.5. 在未限制「交易文件」或雙方當事人所訂關聯基本合約就業務持續所規定之「供應商」義務或 Kyndryl 權利之前提下，「供應商」應依所記載之風險管理準則，就業務與 IT 持續及災難回復等要件分別評量對「Kyndryl 技術」進行「處置」時所使用之各「服務」與「交付項目」及 IT 系統。在前述風險評估保證範圍內，「供應商」應確保前揭各該「服務」與「交付項目」及 IT 系統已依據「業界實作典範」，針對業務與 IT 持續及災難回復計劃，分別予以定義、記載、維護及每年查核。「供應商」應確保前揭計劃之設計，旨在達成以下第 5.6 節所定特定回復時間。

5.6. 「代管服務」有關特定回復點目標 ("**RPO**") 與回復時間目標 ("**RTO**")：24 小時 RPO 及 24 小時 RTO；惟於 Kyndryl 以書面通知「供應商」有關 Kyndryl 已承諾「客戶」較短期間之 RPO 或 RTO（電子郵件視同書面）後，「供應商」應即遵循之。茲因前揭目標攸關「供應商」為 Kyndryl 提供之其他所有「服務」，「供應商」應確保其業務持續與災難回復計劃之設計，旨在達成 RPO 與 RTO，俾使「供應商」得以繼續遵循「交易文件」及雙方當事人所訂關聯基本合與及「條款」所規定「供應商」對 Kyndryl 之所有義務，包括「供應商」及時提供測試、支援及維護之義務。

5.7. 「供應商」應於「服務」與「交付項目」，以及對「Kyndryl 技術」進行「處置」時所使用之系統、網路、應用程式及基礎元件範圍內，持續採取專為下列用途設計之措施：對該等服務與「交付項目」及關聯系統、網路、應用程式及基礎元件進行評量、測試及套用資訊安全建議修補程式。「供應商」於其判斷資訊安全建議修補程式為適用且適當時，應依所記載之嚴重性及風險評估準則實作該修補程式。「供應商」對資訊安全建議修補程式之實作，應受其變更管理政策之拘束。

5.8. 若 Kyndryl 有合理依據認為「供應商」提供予 Kyndryl 之軟硬體可能包含侵害性元素，如間諜軟體、惡意軟體或惡意程式碼，「供應商」應即配合 Kyndryl 就 Kyndryl 之疑慮進行調查與補救。

6. 服務之供應

6.1 「供應商」應支援對 Kyndryl 使用者或「客戶」帳戶進行業界一般方法之聯合鑑別，「供應商」對該 Kyndryl 使用者或「客戶」帳戶進行鑑別時（例如：利用 Kyndryl 集中管理多因子「單一登入 (SSO)」、使用 OpenID Connect (OIDC) 或「安全主張標記語言 (Security Assertion Markup Language, SAML)」進行鑑別），應遵循「業界實作典範」。

7. 下包商。在未限制「交易文件」或雙方當事人所訂關聯基本合約就下包商人才留任所規定之「供應商」義務或 Kyndryl 權利之前提下，「供應商」應確保為「供應商」執行工作之下包商已訂定監督管控措施，俾以遵循「條款」要求「供應商」應遵循之規定及應履行之義務。

8. 實體媒體。「供應商」對預定重複使用之實體媒體為重複使用前，將依「業界實作典範」，以安全之方式予以淨化，非預定重複使用之實體媒體，則予以銷毀。

條款 IX：「代管服務之認證與報告」

「供應商」如係提供 Kyndryl「代管服務」者，適用本條款。

1.1 「供應商」應於以下所定期限內取得下列認證或報告：

認證/報告	**時間範圍**
「供應商」所為「代管服務」相關事項： 符合 ISO 27001、資訊技術、安全技術、資訊安全管理系統等標準之認證，此認證係以證明文件獨立稽核員之評量為依據。 **或** 第二類 SOC 2：一種由信譽良好之獨立稽核員作成之報告，用以證明其依第二類 SOC 2 之規定，對「供應商」之系統、控管及作業所為之審查（至少包括安全、機密性及可用度等項目之審查）。	「供應商」應於「交易文件」* 生效日或「設定日」** 後 120 日內取得 ISO 27001 認證，並於其後每隔 12 個月，依據信譽良好獨立稽核員之評量展延一次此認證（各次展延，均應依據當時最新版本標準為之）。 「供應商」應於「交易文件」* 生效日或「設定日」** 後 240 日內取得第二類 SOC 2 報告，並於其後每隔 12 個月取得一份新報告，該報告係由信譽良好之獨立稽核員作成，用以證明其依第二類 SOC 2 之規定，對「供應商」之系統、控管及作業所為之審查（至少包括安全、機密性及可用度等項目之審查）。 *「供應商」係自前揭生效日起提供「代管服務」者。 **「供應商」所假設提供「代管服務」義務之日期。

1.2 「供應商」書面請求，且 Kyndryl 書面核准者，「供應商」得取得與前揭認證或報告同等之認證或報告，惟「供應商」應瞭解上表所訂時限同樣適用於該同等之認證或報告。

1.3 「供應商」應遵循下列規定：(a) 於 Kyndryl 要求時，應即提供前述「供應商」有義務取得之各認證與報告之複本；(b) 應即解決於進行 SOC 2 審查或同等審查時（經 Kyndryl 核准者）所註記之內部控管弱點。

條款X：「配合、查核及補救」

「供應商」如係提供 Kyndryl「服務」或「交付項目」者，適用本條款。

1. 「供應商」之配合

1.1. Kyndryl 合理質疑任何「服務」或「交付項目」於過去、現在及未來有導致網路安全疑慮者，「供應商」應充分配合 Kyndryl 就該疑慮所為詢問，包括及時完整回應所要求之資訊（透過文件、其他記錄、相關「供應商人員」訪談等方式回應）。

1.2. 雙方當事人同意下列事項：(a) 依要求提供彼此進一步資訊；(b) 簽署其他文件並交付彼此；及 (c) 他方當事人為執行此等「條款」及參用此等「條款」之文件之意旨的目的，而合理提出要求之其他行為或情事。例如，於 Kyndryl 要求時，「供應商」應即提供其與「再處理者」與下包商所訂書面契約中以隱私權與安全為重點之條款，包括授與該等「再處理者」與下包商本身對該等契約之存取權限（「供應商」有權授與該權限者）。

1.3. 於 Kyndryl 要求時，「供應商」應即提供相關資訊，敘明其「交付項目」及其元件之製造、開發或以其他方式委外之所在國家/地區。

2. 查核（以下所稱「設施」，指「供應商」代管、處理或以其他方式存取「Kyndryl 著作物」之所在實體位置）

2.1. 「供應商」應保留稽核記錄，以資證明其遵循「條款」。

2.2. Kyndryl 於事前三十日對「供應商」為書面通知後，得由其自己或由外部稽核員，查核「供應商」是否遵循「條款」，包括基於此目的而進入「設施」，惟 Kyndryl 不進入「供應商」對「Kyndryl 資料」進行「處理」所在資料中心，但 Kyndryl 基於善意理由認為進入該等資料中心足以提供相關資訊者，不在此限。「供應商」應配合 Kyndryl 之查核，包括及時完整回應要求資訊（透過文件、其他記錄、相關「供應商人員」訪談等方式回應）。「供應商」得提出其符合經認可之行為規範或經業界認證之證明，或以其他方式提供相關資訊，據以證明確實遵循「條款」，以供 Kyndryl 納入考量。

2.3. 除下列情形外，於 12 個月之期間內所為查核，以一次為限：(a) Kyndryl 擬查核「供應商」對疑慮事項所為補救，而該等疑慮事項係於 12 個月期間之前一查核所致者；或 (b) 已發生「安全侵害」，而 Kyndryl 欲查核該侵害事件是否與遵循義務相關。有前揭情形之一者，Kyndryl 將同於上述第 2.2 節所規定，於事前三十日以書面通知「供應商」，惟須對「安全侵害」為緊急處理者，Kyndryl 得以事前少於三十日之通知後執行查核。

2.4. 主管機關或其他「管控者」得履行第 2.2 節及第 2.3 節中同於 Kyndryl 之權利，惟該主管機關或其他「管控者」應瞭解主管機關得履行其依法所具有之其他權利。

2.5. Kyndryl 有合理依據足以推斷「供應商」未遵循任一「條款」者（不論該依據是否源自依「條款」或其他規定所為查核，均同），「供應商」應即補救其未遵循「條款」之情事。

3. 防偽程式

3.1. 「供應商」之「交付項目」如有包含電子元件者（例如：硬碟機、固態硬碟、記憶體、中央處理器、邏輯裝置或纜線），「供應商」應持續採用記載完備防偽程式，其目的有二，首先是防止「供應商」提供 Kyndryl 偽造元件，此外可立即偵測及補救「供應商」因其錯誤而提供 Kyndryl 偽造元件之情事。對於提供 Kyndryl 電子元件（內含於「供應商」之「交付項目」）之「供應商」的所有供應商，應使其承擔前揭記載完備防偽程式之相同義務。

4. 補救

4.1. 「供應商」未遵循「條款」所定「供應商」義務，致生「安全侵害」者，「供應商」應更正其未遵循義務，並補救「安全侵害」之不良後果，前述更正之履行與不良後果之補救，應依 Kyndryl 合理指示與時程為之。惟「安全侵害」係因「供應商」供應多租戶「代管服務」所致，並後續影響多位「供應商」客戶（包括 Kyndryl），「供應商」應依「安全侵害」之性質，及時以適當方式更正其執行上之缺失，並補救「安全侵害」所致不良後果，同時亦應就 Kyndryl 對該更正與補救之投入給予補償。

4.2. Kyndryl 於其認為適當或必要時，有權參與第 4.1 節所指「安全侵害」之補救，且雙方當事人因前述更正之履行與補救作為，其所生成本與費用，由「供應商」負擔。

4.3. 例如，「安全侵害」有關補救成本與費用可能包括下列作為所生成本與費用，以及為補救「安全侵害」之不良後果所需之成本與費用：偵測及調查「安全侵害」、依適用法律規章判定責任歸屬、為侵害通知、設置及維護電話客服中心、提供信用監控服務與信用恢復服務、重新載入資料、更正產品瑕疵（包括透過「原始碼」或其他開發）、聘僱第三人協助進行前揭或其他相關活動。為求明確，茲進一步說明如下：補救成本與費用不包括 Kyndryl 之利潤、業務、價值、收入、商譽或預期盈餘等之損失。