第 I 条，业务联系信息

供应商或 Kyndryl 处理对方的 BCI 时，本条款适用。

1.1 Kyndryl 和供应商可以在供应商提供服务和可交付成果的任何业务地点处理对方的 BCI。

1.2 一方：

(a) 不会出于任何其他目的使用或披露另一方的 BCI（为清楚起见，任何一方均不会在未经另一方事先书面同意的情况下，出于任何营销目的出售、使用或披露另一方的 BCI，需要时可能还要经受影响数据主体的事先书面同意），以及

(b) 在任何未经授权使用个人信息的情况发生，且一方希望停止处理和补救时，在对方书面要求下，将立即删除、修改、纠正、退回对方的 BCI，或提供有关处理对方 BCI 或限制处理对方 BCI 的信息，或对对方 BCI 采取任何其他合理要求的措施。

1.3 双方未就双方的 BCI 达成联合控制者关系，并且交易文件中的任何规定均不得解释为指示建立联合控制者关系的任何意图。

1.4 Kyndryl 隐私声明（位于 https://www.kyndryl.com/us/en/privacy）包含 Kyndryl 处理 BCI 的更多详细信息。

1.5 双方已实施并将维护技术和组织安全措施，以保护对方的 BCI 免遭丢失、破坏、变更、意外或未经授权的披露、意外或未经授权的访问以及非法处理。

1.6 供应商在发现任何涉及 Kyndryl BCI 的安全违规后，应立即（并且在任何情况下不迟于 48 小时）通知 Kyndryl。供应商将通过 cyber.incidents@kyndryl.com 提供此类通知。供应商将提供 Kyndryl 合理请求的信息，包括有关此类安全违规的信息，以及供应商采取的任何补救和恢复活动的状态。合理请求的信息主要涉及安全违规情况或供应商所采取的补救和恢复活动，例如，用于表明针对设备、系统或应用的特权访问权限、管理员访问权限和其他访问权限的日志；设备、系统或应用的取证图像；以及其他事项。

1.7 如果供应商仅处理 Kyndryl 的 BCI，且无权访问任何其他类型的数据或材料或任何 Kyndryl 公司系统，则本条和第 X 条（合作、验证和补救）是唯一适用于此类处理的条款。

第 II 条，技术和组织措施，数据安全性

如果供应商处理 Kyndryl 的 BCI 以外的 Kyndryl 数据，则本条款适用。供应商将在提供所有服务和可交付成果时遵守本条款的要求，并以此保护 Kyndryl 数据免遭丢失、破坏、更改、意外或未授权披露、意外或未授权获取以及非法处理。本条款要求扩展到供应商在提供可交付成果和服务时操作或管理的所有 IT 应用程序、平台和基础架构，包括所有开发、测试、托管、支持、操作和数据中心环境。

1. 数据使用

1.1 未经 Kyndryl 事先书面同意，供应商不得将任何其他信息或数据（包括任何个人数据）添加到 Kyndryl 数据中，也不得在 Kyndryl 数据中包含任何其他信息或数据，并且供应商不得出于除提供服务和可交付成果以外的任何其他目的，以任何方式（汇总或其他形式）使用 Kyndryl 数据（例如，不允许供应商使用或重复使用 Kyndryl 数据来评估供应商产品的有效性或改进供应商产品或服务，以研发创建新产品或生成有关供应商产品的报告）。除非交易文件中明确允许，否则禁止供应商出售 Kyndryl 数据。

1.2 除非交易文件中明确允许，否则供应商将不会在交付成果中或作为服务的一部分嵌入任何 Web 跟踪技术（此类技术包括 HTML5、本地存储、第三方标签或令牌以及 Web 信标）。

2. 第三方请求和保密

2.1 除非得到 Kyndryl 事先书面授权，否则供应商不得将 Kyndryl 数据透露给任何第三方。如果政府（包括任何监管机构）要求访问 Kyndryl 数据（例如，如果美国政府向供应商发出国家安全命令以获取 Kyndryl 数据），或者法律另外要求披露 Kyndryl 数据，则供应商将以书面形式通知 Kyndryl 此类要求，并为 Kyndryl 提供合理的机会对任何披露提出异议（在法律禁止通知的情况下，供应商将采取其合理认为适当的步骤，通过司法行动或其他方式对 Kyndryl 数据的禁止和披露提出异议）。

2.2 供应商向 Kyndryl 保证：(a) 只有需要访问 Kyndryl 数据以提供服务或可交付成果的员工才能访问，并仅在提供这些服务和可交付成果所必需的范围内进行访问；(b) 其员工有保密义务，要求员工仅在此类条款允许的范围内使用和披露 Kyndryl 数据。

3. 归还或删除 Kyndryl 数据

3.1 在交易文件终止或到期时，供应商将根据 Kyndryl 选择删除或归还 Kyndryl 数据，或按 Kyndryl 要求提前删除或归还。如果 Kyndryl 要求删除，则供应商将遵循行业最佳实践，使数据不可读且无法重组或重建，并向 Kyndryl 证明此类删除。如果 Kyndryl 要求归还 Kyndryl 数据，则供应商将按 Kyndryl 的合理安排，遵照 Kyndryl 的合理书面说明进行归还。

第III 条，隐私

如果供应商处理 Kyndryl 个人数据，则本条款适用。

1. 处理

1.1 Kyndryl 任命供应商为处理 Kyndryl 个人数据的处理机构，其唯一目的是按照 Kyndryl 的指示（包括这些条款、交易文件和双方之间相关基本协议中的指示）提供可交付成果和服务。如果供应商未遵从某条指示，Kyndryl 可以书面通知的方式终止受影响的部分服务。如果供应商认为某条指示违反了数据保护法律，则供应商应在法律要求的任何时间范围内及时通知 Kyndryl。如果供应商因未能履行其在此类条款下的任何义务，导致未经授权使用个人信息，一般而言，在任何情况下未经授权使用个人信息，Kyndryl 将有权停止处理，纠正并补救未经授权使用带来的有害影响，且此类行动和补救措施将按照 Kyndryl 的合理指示和安排进行。

1.2 供应商将遵守适用于服务和可交付成果的所有数据保护法律。

1.3 交易文件的附录或交易文件本身列出了以下 Kyndryl 数据相关内容：

(a) 数据主体类别；
(b) Kyndryl 个人数据的类型；
(c) 数据操作和处理活动；
(d) 处理的持续时间和频率；以及
(e) 分包处理机构列表。

2. 技术和组织措施

2.1 供应商将实施和维护第 II 条（技术和组织措施，数据安全性）和第 VIII 条（技术和组织措施，一般安全性）中规定的技术和组织措施，并以此确保与其服务和可交付成果所面临风险相对应的安全级别。供应商证明自己理解并将遵守第 II 条、第 III 条和第 VIII 条中的限制。

3. 数据主体权利和请求

3.1 若数据主体发出任何行使有关 Kyndryl 个人数据的任何数据主体权利（例如，纠正、删除或阻止数据）的请求，供应商将（按照允许 Kyndryl 和任何其他控制者履行其法律义务的安排）立即通知 Kyndryl。供应商还可以立即将提出此类请求的数据主体指示给 Kyndryl。除非法律要求或 Kyndryl 提出书面指示，否则供应商将不会答复数据主体的任何请求。

3.2 如果 Kyndryl 有义务向其他控制者或其他第三方（例如，数据主体或监管者）提供有关 Kyndryl 个人数据的信息，则供应商将通过提供信息并采取 Kyndryl 要求的其他合理行动为 Kyndryl 提供协助，支持 Kyndryl 及时响应此类其他控制者或第三方。

4. 分包处理机构

4.1 在添加新的分包处理机构或通过现有分包处理机构扩展处理范围之前，供应商将事先向 Kyndryl 发出书面通知，该书面通知将标识分包处理机构的名称并描述新的或扩展的处理范围。Kyndryl 可以随时以合理的理由反对任何此类新的分包处理机构或扩展范围，如果反对，则各方将本着诚信协作的原则来处理 Kyndryl 的异议。若 Kyndryl 在供应商书面通知之日起 30 天内未提出异议，供应商将委托新的分包处理机构或扩展现有分包处理机构的处理范围，但 Kyndryl 有权随时提出异议。

4.2 在分包处理机构处理任何 Kyndryl 数据之前，供应商将对每个已批准的分包处理机构履行此类条款中规定的数据保护、安全性和认证义务。对于每个分包处理机构的义务履行，供应商应对 Kyndryl 承担全部责任。

5. 跨境数据处理

在使用时：

已通过充分性认证的国家/地区指根据适用的数据保护法律或监管机构的决定就相关的数据传输提供适当数据保护级别的国家/地区。

数据进口商指并非在已通过充分性认证的国家/地区设立的处理机构或分包处理机构。

欧盟标准合同条款（以下简称"欧盟 SCC"）指除第 9(a) 条选项 1 和第 17 条选项 2 外，适用的附带可选条款的《欧盟标准合同条款》（欧委会决议 2021/914），已正式发布于 https://commission.europa.eu/publications/standard-contractual-clauses-international-transfers_en

塞尔维亚标准合同条款（以下简称"塞尔维亚 SCC"）指"塞尔维亚公共重要信息和个人数据保护专员"通过的《塞尔维亚标准合同条款》，已发布于 https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx。

标准合同条款（以下简称"**SCC**"）指适用的数据保护法律要求的合同条款，适用于将个人数据传输到并非在通过充分性认证的国家/地区设立的处理机构。

《欧盟委员会标准合同条款之英国国际数据传输附录》（以下简称《英国附录》）是指针对《欧盟委员会标准合同条款》的《英国国际数据传输附录》，正式发布于 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/。

《欧盟委员会标准合同条款瑞士附录》（"瑞士附录"）是指依据瑞士数据保护局 ("**FDPIC**") 的决定及根据《瑞士联邦数据保护法案》("**FADP**") 所适用的《欧盟委员会标准合同条款》的合同条款。

5.1 未经 Kyndryl 事先书面同意，供应商不得跨境转移或披露（包括通过远程访问）任何 Kyndryl 个人数据。如果 Kyndryl 提供此类同意，双方将合作确保遵守适用的数据保护法律。如果这些法律要求 SCC，则供应商将应 Kyndryl 的要求立即达成 SCC。

5.2 关于欧盟 SCC：

(a) 如果供应商并非在已通过充分性认证的国家/地区设立：供应商特此作为进口商，与 Kyndryl 签订欧盟 SCC，且供应商将根据欧盟 SCC 第 9 条与每家经批准分包处理机构签订书面协议，并将在请求时向 Kyndryl 提供这些协议的副本。

(i) 除非双方另有书面协议，否则欧盟 SCC 的模块 1 不适用。

(ii) 欧盟 SCC 的模块 2 适用于 Kyndryl 是控制者的情况，模块 3 适用于 Kyndryl 是处理机构的情况。根据欧盟 SCC 第 13 条，当模块 2 或模块 3 适用时，双方同意 (1) 欧盟 SCC 将受主管监管机构所在地的欧盟成员国法律管辖，以及 (2) 欧盟 SCC 引起的任何争议将由主管监管机构所在地的欧盟成员国法院审理。如果第 (1) 中的此类法律不允许第三方受益人权利，那么欧盟 SCC 应受荷兰法律管辖，而第 (2) 条中欧盟 SCC 引起的任何争议应由荷兰阿姆斯特丹法院裁决。

(b) 如果供应商和 Kyndryl 双方均在已通过充分性认证的国家/地区设立，则供应商将作为数据出口商，与位于未通过充分性认证的国家/地区的每家经批准分包处理机构签订欧盟 SCC。供应商应执行所需的传输影响评估 (TIA)，并立即通知 Kyndryl (1) 是否需要采取补充措施以及 (2) 已采取的措施。在请求时，供应商应向 Kyndryl 提供 TIA 结果以及理解和评估结果所需的任何信息。如果 Kyndryl 不同意供应商 TIA 的结果或采取的补充措施，Kyndryl 和供应商将合作确定可行的解决方案。Kyndryl 有权在没有补偿的情况下暂停或终止供应商的相关服务。为避免疑义，这并不能免除供应商的分包处理机构与 Kyndryl 或其客户成为欧盟 SCC 一方的责任，如下文第 5.2 (d) 节所述。

(c) 如果供应商在欧洲经济区设立，而 Kyndryl 是不受通用数据保护条例 2016/679 约束的控制者，则适用欧盟 SCC 模块 4，供应商特此作为数据出口商与 Kyndryl 签订欧盟 SCC。如果欧盟 SCC 的模块 4 适用，双方同意欧盟 SCC 受荷兰法律管辖，因欧盟 SCC 引起的任何争议应由荷兰阿姆斯特丹法院裁决。

(d) 如果其他控制者（例如客户或关联公司）根据第 7 条中的“对接条款”请求成为欧盟 SCC 的一方，供应商特此同意任何此类请求。

(e) 完成欧盟 SCC 附录 II 所需的技术和组织措施可在本协议条款、交易文件本身以及双方之间的相关基础协议中找到。

(f) 如果欧盟 SCC 与本条款之间存在任何冲突，则以欧盟 SCC 为准。

5.3 关于《英国附录》：

(a) 如果供应商并非在已通过充分性认证的国家/地区成立：(i) 供应商特此作为进口商，与 Kyndryl 签订《英国附录》，以附加到上述欧盟 SCC 中（根据处理活动的具体情况确定是否适用）；以及 (ii) 供应商将与每个获得批准的分处理机构签订书面协议，并根据要求向 Kyndryl 提供这些协议的副本。

(b) 如果供应商在已通过充分性认证的国家/地区成立，并且 Kyndryl 是不受《英国通用数据保护条例》（根据 2018 年欧盟（退出）法案纳入英国法律）约束的控制者，那么供应商特此作为出口商与 Kyndryl 签订《英国附录》，以附加到上文第 5.2(b) 节中规定的欧盟 SCC 中。

(c) 如果其他控制者（例如客户或关联公司）请求成为《英国附录》的一方，供应商特此同意任何此类请求。

(d) 《英国附录》中的附录信息（如表 3 所列）可在适用的欧盟 SCC、本协议条款、交易文件本身以及双方之间的相关基础协议中找到。当《英国附录》发生变更时，Kyndryl 和供应商均不得终止《英国附录》。

(e) 如果《英国附录》与本协议条款之间存在任何冲突，则以《英国附录》为准。

5.4 关于塞尔维亚 SCC：

(a) 如果供应商并非在已通过充分性认证的国家/地区设立：(i) 供应商将作为处理机构，特此代表自己与 Kyndryl 签订塞尔维亚 SCC；(ii) 供应商将根据塞尔维亚 SCC 第 8 条与每家经批准分包处理机构签订书面协议，并将在请求时向 Kyndryl 提供这些协议的副本。

(b) 如果供应商在已通过充分性认证的国家/地区设立，则供应商特此代表位于未通过充分性认证的国家/地区的每家分包处理机构与 Kyndryl 签订塞尔维亚 SCC。如果供应商无法对任何此类分包处理机构执行此操作，则在允许分包处理机构处理任何 Kyndryl 个人数据之前，供应商将向 Kyndryl 提供该分包处理机构签署的塞尔维亚 SCC，以供 Kyndryl 会签。

(c) 根据实际需要，Kyndryl 和供应商之间的塞尔维亚 SCC 将作为控制者和处理机构之间的塞尔维亚 SCC，或作为“处理机构”和“分包处理机构”之间的背靠背书面协议。如果塞尔维亚 SCC 与本条款之间存在任何冲突，则以塞尔维亚 SCC 为准。

(d) 完成塞尔维亚 SCC 附录 1 至 8（其目的是管理向未通过充分性认证的国家/地区传输个人数据）所需的信息可在本协议条款、交易文件的附录或交易文件本身中找到。

5.5. 关于《瑞士附录》：

(a) 若依据第 5.1 条对 Kyndryl 个人数据的传输 受《瑞士联邦数据保护法案》("FADP") 的管辖，则在本条款第 5.2 条约定的欧盟 SCC 应适用于此类数据传输，并应实施下列修订，以便针对瑞士个人数据执行 GDPR 标准：

- 提及《通用数据保护条例》("GDPR") 亦应视为提及 FADP 的等效条文。
- 瑞士联邦数据保护信息委员会是第 13 条和附件 I 所述的有关主管机关。欧盟 SCC 的 C
- 若数据传输受 FADP 独家管辖，则以瑞士法律作为管辖法律，且
- 欧盟 SCC 第 18 条所述的"成员国"应延伸至包含瑞士在内，以方便瑞士数据主体在其惯常居所行使自身权利。

(b) 为免生疑义，前述内容均无意以任何方式降低欧盟 SCC 规定之数据保护级别，只是将此等保护级别延伸至瑞士数据主体。若情况并非如此，则以欧盟 SCC 为准。

6. 协助和记录

6.1 考虑到数据处理的性质，供应商将采取适当的技术和组织措施来协助 Kyndryl 履行与数据主体请求和权利相关的义务。考虑到供应商可用的信息，供应商还将协助 Kyndryl 确保履行有关处理安全性、安全违规行为的通知和通信以及创建数据保护影响评估有关的义务，包括事先咨询负责的监管机构。

6.2 供应商将保留每个分包处理机构的名称和联系方式的最新记录，包括每个分包处理机构的代表和数据保护人员。根据要求，供应商将按计划向 Kyndryl 提供此记录，从而让 Kyndryl 及时响应客户或其他第三方的任何需求。

第 IV 条，技术和组织措施，代码安全性。

如果供应商可以访问 Kyndryl 源代码，则本条款适用。供应商将遵守本条款的要求，并以此保护 Kyndryl 源代码，使其免遭丢失、破坏、更改、意外或未经授权的披露，意外或未经授权的访问以及非法的处理形式。本条款要求扩展到供应商在提供可交付成果和服务以及在处理 Kyndryl 技术时操作或管理的所有 IT 应用程序、平台和基础架构，包括所有开发、测试、托管、支持、操作和数据中心环境。

1. 安全性要求

如下所示，

禁止的国家/地区指任何国家/地区：(a) 根据 2019 年 5 月 15 日《确保信息和通信技术与服务供应链安全的行政命令》，美国政府确定的外敌，(b)《 2019 年美国国防授权法》第 1654 条列出的国家/地区，或 (c) 在交易文件中确定为“禁止的国家/地区”。

1.1 供应商不得向任何第三方分发 Kyndryl 源代码，也不得将 Kyndryl 源代码交由任何第三方保管。

1.2 供应商不允许任何 Kyndryl 源代码放置于禁止的国家/地区的服务器上。无论有任何理由，供应商均不允许位于被禁止的国家/地区或访问被禁止的国家/地区的任何人（包括自己的员工）访问或使用任何 Kyndryl 源代码，不管该 Kyndryl 源代码位于全球任何地方，并且供应商不允许在任何需要此类访问或使用的禁止的国家/地区开展任何开发、测试或其他工作。

1.3 在法律或法律解释要求向任何第三方披露源代码的任何司法管辖区中，供应商均不得保管或分发 Kyndryl 源代码。如果 Kyndryl 源代码所在的司法管辖区发生法律变更或法律解释，可能因此要求供应商向第三方披露该源代码，则供应商应立即销毁该 Kyndryl 源代码或将其从该司法管辖区内删除，并且如果此类法律或法律解释继续有效，则不得将任何其他 Kyndryl 源代码保管于该司法管辖区中。

1.4 根据 2019 年美国国防授权法第 1654 或 1655 条，供应商将不会直接或间接采取任何行动（包括订立任何协议），让供应商、Kyndryl 或任何第三方承担披露义务。为了清楚起见，除非交易文件或当事方之间的相关基本协议中明确允许的情况外，未经 Kyndryl 事先书面同意，任何情况下均不允许供应商向任何第三方披露 Kyndryl 源代码。

1.5 如果 Kyndryl 通知供应商，或第三方通知任何一方：(a) 供应商已允许将 Kyndryl 源代码带入禁止的国家/地区或上述 1.3 条所述的任何司法管辖区，(b) 供应商以其他方式发布、访问或以交易文件或各方间的相关基本协议或其他协议所不允许的方式使用 Kyndryl 源代码，或 (c) 供应商违反了上述第 1.4 条，则在交易文件或各方间的相关基本协议或其他协议议下，Kyndryl 处理此类不合乎法律或衡平法事宜的权利不受限制：(i) 如果此类通知是发给供应商的，则供应商立即与 Kyndryl 分享该通知；(ii) 供应商遵照 Kyndryl 与供应商协商后合理确定的安排，在 Kyndryl 的合理指示下进行调查和补救。

1.6 如果 Kyndryl 有理由认为可能需要更改供应商有关源代码访问的政策、程序、控制或做法，以解决网络安全、知识产权被盗或者类似或相关的风险（包括在不进行此类更改的情况下可能会对 Kyndryl 造成的风险，如限制 Kyndryl 向某些客户进行销售或进入某些市场，或无法满足客户安全或供应链需求），那么 Kyndryl 可以联系供应商，以讨论解决此类风险所需的操作，包括对此类政策、程序、控制或做法的更改。应 Kyndryl 的要求，供应商将与 Kyndryl 合作，评估是否有必要进行此类更改并实施适当的、双方同意的更改。

第 V 条，安全开发

如果供应商将向 Kyndryl 提供其或第三方源代码或本地软件，或供应商的任何可交付成果或服务将作为 Kyndryl 产品或服务的一部分提供给 Kyndryl 客户，则本条款适用。

1. 安全准备情况

1.1 供应商将与 Kyndryl 的内部流程合作，以评估依赖于任何供应商可交付成果的 Kyndryl 产品和服务的安全准备情况，包括通过文件、其他记录、相关供应商人员的采访或类似项目。

2. 安全开发

2.1 本第 2 条仅适用于供应商向 Kyndryl 提供本地软件的情况。

2.2 供应商已按照行业最佳实践，在交易文件有效期内实施并将在整个交易文件有效期内维持网络、平台、系统、应用程序、设备、物理基础设施、事件响应和以人员为重点的安全政策、程序和控制，以保护：(a) 供应商或供应商聘用的任何第三方为或就可交付成果操作、管理、使用或以其他方式依赖的开发、构建、测试和操作系统与环境，以及 (b) 所有可交付成果源代码，使其免遭丢失、非法的处理形式以及未经授权的访问、披露或更改。

3. ISO 20243 认证

3.1 本第 3 条仅适用于供应商的任何可交付成果或服务将作为 Kyndryl 产品或服务的一部分提供给 Kyndryl 客户的情况。

3.2 供应商将获得以下标准认证：ISO 20243、信息技术、开放可信技术供应商标准 (O-TTPS)、减轻恶意污染和假冒产品的认证（自行评估或由信誉良好的独立审核员评估得出的认证）。或者，如果供应商提出书面要求，Kyndryl 书面批准，则供应商将获得基本等效的安全开发和供应链实践行业标准的合规证明（在 Kyndryl 批准的情况下，自行评估或由信誉良好的独立审核员评估得出的认证）。

3.3 供应商应在交易文件生效后 180 天内获得符合 ISO 20243 或基本等效行业标准的认证（如果 Kyndryl 书面批准），
之后每 12 个月更新一次认证（每次更新均以当时最新版本的适用标准为准，即 ISO 20243，或者，如果 Kyndryl 已书面批准，则以针对安全开发和供应链实践的基本等效行业标准为准）。

3.4 按照以上第 2.1 条和第 2.2 条的规定，供应商将在要求时立即向 Kyndryl 提供一份认证副本。

4. 安全漏洞

如下所示，

错误纠正指纠正可交付成果中的错误或缺陷（包括安全漏洞）的漏洞修复和修正。

缓解措施指减轻或避免安全漏洞风险的任何已知措施。

安全漏洞指可交付成果在设计、编码、开发、实施、测试、运行、支持、维护或管理中的一种状态，这种状态可能受到任何人的攻击从而导致未经授权的访问或利用，包括：(a) 访问以控制或破坏系统的运行，(b) 访问以删除、更改或提取数据，或者 (c) 更改用户或管理员的身份、授权或许可。无论是否为其分配通用漏洞与披露 (CVE) ID 或者任何评分或官方分类，都可能存在安全漏洞。

4.1 供应商声明并保证其将 (a) 使用当时最新的行业标准最佳实践来识别安全漏洞，包括通过持续的静态和动态源代码应用程序安全扫描、开源安全扫描和系统漏洞扫描，以及 (b) 遵守此类条款的要求，帮助预防、检测和纠正可交付成果以及供应商在其中或通过其创建和提供服务及可交付成果的所有 IT 应用程序、平台和基础架构中的安全漏洞。

4.2 如果供应商意识到了可交付成果或任何此类 IT 应用程序、平台或基础架构中的安全漏洞，那么供应商应根据下表中定义的严重性级别和时间范围向 Kyndryl 提供所有版本和发行版的可交付成果

的错误纠正和缓解措施：

严重性级别*
紧急安全漏洞 – 指构成严重潜在全球威胁的安全漏洞。Kyndryl 自行指定紧急安全漏洞，而不考虑 CVSS 基本评分。
严重 – 指 CVSS 基本分数在 9 - 10.0 之间的安全漏洞
高级 – 指 CVSS 基本分数在 7.0 - 8.9 之间的安全漏洞
中级 – 指 CVSS 基本分数在 4.0 - 6.9 之间的安全漏洞
低级 – 指 CVSS 基本分数在 0.0 - 3.9 之间的安全漏洞

时间范围				
紧急	***严重***	***高级***	***中级***	***低级***
4 天或更短时间（由 Kyndryl 首席信息安全办公室确定）	30 天	30 天	90 天	根据行业最佳实践

* 如果安全漏洞没有立即分配的 CVSS 基本分数，那么供应商将应用与此类漏洞的性质和情况相适应的严重性级别。

4.3 对于已公开披露但供应商尚未向 Kyndryl 提供任何错误纠正或缓解措施的安全漏洞，供应商应实施任何在技术上可行的附加安全控制措施，以便缓解此类漏洞的风险。

4.4 如果 Kyndryl 不满意供应商对上述交付成果或任何应用程序、平台或基础架构中的任何安全漏洞的响应措施，那么在不损害 Kyndryl 享有的任何其他权利的情况下，供应商应立即安排 Kyndryl 直接与负责错误纠正的供应商副总裁或同等级别管理人员讨论 Kyndryl 的问题。

4.5 安全漏洞的示例包括第三方代码或服务终止 (EOS) 开源代码，这些类型的代码不再接收安全修订包。

第VI 条，企业系统的访问

如果供应商员工可以访问任何企业系统，则本条款适用。

1. 通用条款

1.1 Kyndryl 将决定是否授权供应商员工访问企业系统。如果 Kyndryl 授权，则供应商将遵守本条款的要求，并且具有此访问权限的员工也应遵守该条款的要求。

1.2 Kyndryl 将确定供应商员工访问企业系统的方式，包括这些员工将通过 Kyndryl 还是供应商提供的设备访问企业系统。

1.3 供应商员工只能访问企业系统，并且只能使用 Kyndryl 授予该访问权限的设备来提供服务。供应商员工不得使用 Kyndryl 授权的设备向任何其他个人或实体提供服务，或访问任何供应商或第三方 IT 系统、网络、应用程序、网站、电子邮件工具、协作工具等，或与此类服务有关的其他内容。

1.4 为了清楚起见，供应商员工不得出于任何个人原因使用 Kyndryl 授权访问企业系统的设备（例如，供应商员工不得在此类设备上存储音乐、视频、图片等个人文件，也不得出于个人原因使用此类设备中的网络）。

1.5 未经 Kyndryl 事先书面许可，供应商员工不得复制可通过企业系统访问的 Kyndryl 材料（也不得将任何 Kyndryl 材料复制到便携式存储设备，例如 USB、外部硬盘等）。

1.6 根据要求，供应商将通过员工姓名确认其员工有权访问并已经在 Kyndryl 确定的时间内访问的特定企业系统。

1.7 在有权访问任何企业系统的任何供应商员工不再：(a) 与供应商有雇佣关系，或 (b) 从事需要此类访问的活动时，供应商应在二十四 (24) 小时内通知 Kyndryl。供应商将与 Kyndryl 合作，确保立即撤销此类前任或现任员工的访问权限。

1.8 供应商应立即向 Kyndryl 报告任何实际或可疑的安全事件（例如，Kyndryl 或供应商设备丢失，或对设备或数据、材料或其他信息的未经授权访问），并与 Kyndryl 合作调查此类事件。

1.9 未经 Kyndryl 事先书面同意，供应商不得允许任何代理商、独立承包商或转包商员工访问任何企业系统；如果 Kyndryl 表示同意，则供应商将按照合同约定，保证这些人员及其雇主像供应商员工一样遵守本条款的要求，并为此类人员或雇主采取的有关此类企业系统访问的任何行动和疏忽对 Kyndryl 负责。

2. 设备软件

2.1 供应商将指示其员工及时安装 Kyndryl 所要求的所有设备软件，以便安全访问企业系统。供应商及其员工均不得干扰该软件的操作或该软件启用的安全功能。

2.2 供应商及其员工将遵守 Kyndryl 设置或使用的设备配置规则，并以其他方式与 Kyndryl 合作，以帮助确保软件按 Kyndryl 预期的方式运行。例如，供应商将不会覆盖软件网站阻止或自动修补功能。

2.3 供应商员工不得与任何其他人共享用于访问企业系统的设备，或其设备用户名、密码等。

2.4 如果 Kyndryl 授权供应商员工使用供应商设备访问企业系统，则供应商将在 Kyndryl 批准的设备上安装并运行操作系统，并将在 Kyndryl 指示的合理时间内升级到该操作系统的新版本或新操作系统。

3. 监督与合作

3.1 Kyndryl 拥有以任何方式，在任何地点，以 Kyndryl 认为有必要或适当的方式监视和补救潜在入侵和其他网络安全威胁的无条件权利，无需事先通知供应商或任何供应商员工或其他人员。此类权利的示例：Kyndryl 可以随时 (a) 在任何设备上执行安全测试，(b) 监视、通过技术或其他手段进行恢复，并审查通信（包括来自任何电子邮件帐户的电子邮件）、记录、文件以及存储在任何设备中或通过任何企业系统传输的其他项目，以及 (c) 获取任何设备的完整取证图像。如果 Kyndryl 需要供应商来合作行使其权利，则供应商需全力配合并及时满足 Kyndryl 的合作请求（包括，例如，安全配置任何设备的请求，在任何设备上安装监视软件或其他软件的请求，共享系统级连接详细信息的请求，在任何设备上采取事件响应措施，并提供对任何设备的物理访问权，以便 Kyndryl 获得完整的取证图像等，以及类似和相关的请求）。

3.2 如果 Kyndryl 认为出于保护 Kyndryl 的目的有必要这样做，那么 Kyndryl 可以随时撤消任何供应商员工或所有供应商员工对企业系统的访问权，而无需事先通知供应商或任何供应商员工或其他人员。

3.3 交易文件的任何规定及双方之间相关的基本协议或任何其他协议，包括可能需要数据、资料或其他信息仅位于一个或多个选定位置的任何规定，或者可能要求只有选定位置的人员才可以访问此类数据、材料或其他信息的规定，均不会以任何方式阻止、减少或限制 Kyndryl 的权利。

4. Kyndryl 设备

4.1 Kyndryl 将保留所有 Kyndryl 设备的所有权，由供应商承担设备丢失（包括盗窃、故意破坏或过失引起设备丢失）的风险。未经 Kyndryl 事先书面同意，供应商不得对 Kyndryl 设备进行任何更改，包括对设备软件、应用程序、安全性设计、安全性配置，或物理、机械或电气设计的任何更改。

4.2 供应商将于无需这些设备再提供服务后的 5 个工作日内退还所有 Kyndryl 设备，并且如果 Kyndryl 要求，同时销毁这些设备上的所有数据、材料和其他任何形式的其他信息，且不会保留任何副本，按照行业最佳实践永久删除所有此类数据、材料和其他信息。供应商将以交付时相同状况（合理的磨损除外）包装和退还 Kyndryl 设备，但需要自费将其运送到 Kyndryl 指定的位置。供应商未能遵守第 4.2 条中的任何一项义务，均构成对交易文件和双方间的基本协议及任何相关协议的重大违规，"相关"协议指的是对任何企业系统的访问便于供应商遵照该协议执行任务或其他活动。

4.3 Kyndryl 将为 Kyndryl 设备提供支持（包括设备检查以及预防性和补救性维护）。供应商将立即向 Kyndryl 提出补救服务需求。

4.4. 对于 Kyndryl 拥有或有权许可的软件程序，Kyndryl 授予供应商临时使用、存储和制作足够数量副本的权利，以支持其对 Kyndryl 设备的授权使用。供应商不得将程序转让给任何人，不得复制软件许可信息，也不得反汇编、反编译、反向工程或以其他方式转换任何程序，除非适用法律明确许可，且无豁免合同的可能性。

5. 更新

5.1 尽管双方之间的交易文档或相关基本协议中有相反规定，在书面通知供应商后，且无需征得供应商同意，Kyndryl 即可更新、补充或以其他方式修改本条款，以满足适用法律或客户义务的要求，并反映安全最佳实践的任何进展，或者 Kyndryl 认为保护企业系统或 Kyndryl 所必需的其他方式。

第 VII 条，员工扩充

若供应商员工会投入全部工作时间来为 Kyndryl 提供服务，在 Kyndryl 场所、客户场所或在家中执行所有这些服务，并且仅利用 Kyndryl 设备访问企业系统来提供服务，则本条款适用。

1. 访问企业系统；Kyndryl 的环境

1.1 供应商只能使用 Kyndryl 提供的设备访问企业系统，以执行服务。

1.2 对于企业系统的所有访问，供应商将遵守第 VI 条（企业系统的访问）中列出的条款。

1.3 供应商及其员工只能通过 Kyndryl 供应的设备来提供服务，并且这些设备只能由供应商及其员工使用以提供服务。为了清楚起见，在任何情况下，供应商或其员工均不得使用任何其他设备来提供服务，也不得将 Kyndryl 设备用于任何其他供应商客户，或用于向 Kyndryl 提供服务以外的任何目的。

1.4 使用 Kyndryl 设备的供应商员工可以彼此共享 Kyndryl 材料，并在 Kyndryl 设备上存储这些材料，但仅限于成功提供服务所必需的此类共享和存储。

1.5 除在 Kyndryl 设备中进行此类存储外，供应商或其员工在任何情况下均不得从 Kyndryl 保存材料所用的 Kyndryl 信息库、环境、工具或基础架构中删除任何 Kyndryl 材料。

1.6 为清楚起见，未经 Kyndryl 事先书面同意，不会授权供应商及其员工将任何 Kyndryl 材料转移到任何供应商存储库、环境、工具或基础架构或任何其他供应商系统、平台、网络等。

1.7 第 VIII 条（技术和组织措施，一般安全性）不适用于供应商的服务，其中供应商员工会投入全部工作时间来为 Kyndryl 提供服务，在 Kyndryl 场所、客户场所或在家中执行所有这些服务，并且仅利用 Kyndryl 设备访问企业系统来提供服务。除此之外，第 VIII 条适用于供应商服务。

第 VIII 条，技术和组织措施，一般安全性

如果供应商向 Kyndryl 提供任何服务或可交付成果，则本条款适用，除非供应商仅在提供这些服务和可交付成果时有权访问 Kyndryl BCI（即，供应商将不会处理任何其他 Kyndryl 数据或无法访问任何其他 Kyndryl 材料或任何企业系统）、供应商的服务和可交付成果仅限向 Kyndryl 提供本地软件，或供应商根据第 VII 条（包括第 1.7 条）以员工扩充模式提供其所有服务和可交付成果。

供应商将遵守本条的要求，并以此保护：(a) Kyndryl 材料免遭丢失、破坏、变更、意外或未经授权的披露以及意外或未经授权的访问；(b) Kyndryl 不会遭到非法形式的处理，以及 (c) Kyndryl 技术不会遭到非法形式的处理。本条款要求扩展到供应商在提供可交付成果和服务以及在处理 Kyndryl 技术时操作或管理的所有 IT 应用程序、平台和基础架构，包括所有开发、测试、托管、支持、操作和数据中心环境。

1. 安全策略

1.1 供应商应维护和遵守供应商业务不可或缺的并且所有供应商人员必须遵守的 IT 安全策略和实践，并与行业最佳实践保持一致。

1.2 供应商应至少每年审查一次其 IT 安全策略和实践，并在供应商认为必要的时候进行修订，以保护 Kyndryl 材料。

1.3 对于所有新雇员，供应商均维护并遵循标准强制性雇佣证明要求，并将此类要求推广至所有供应商人员和供应商全资子公司。这些要求将包括当地法律允许范围内的犯罪背景调查、身份验证证明以及供应商认为必要的其他调查。供应商应在其认为必要时定期重申并重新验证这些要求。

1.4 供应商应每年为其雇员提供安全和隐私培训，并要求所有雇员每年确认他们将会遵守供应商行为准则或类似文档中规定的供应商道德与商业行为准则、保密和安全策略。供应商应向拥有服务、可交付成果或 Kyndryl 材料的任何组件的管理权限的人员提供额外的策略和流程培训，这类培训特定于他们的角色和对服务、可交付成果和 Kyndryl 材料的支持，并在必要时维护所需的合规性和认证。

1.5 供应商将设计安全和隐私措施，以保护和维护 Kyndryl 材料的可用性，包括通过其实施、维护和遵守所有服务和可交付成果以及所有 Kyndryl 技术的处理在设计、安全工程和安全操作上需要安全和隐私的策略和程序。

2. 安全事件

2.1 供应商应维护并遵循与有关计算机安全性事件处理的行业最佳实践相一致的书面事件响应策略。

2.2 供应商将对 Kyndryl 材料的未经授权的访问或未经授权的使用进行调查，并将定义并执行适当的响应计划。

2.3 供应商在发现任何安全违规后，应立即（并且在任何情况下不迟于 48 小时）通知 Kyndryl。供应商将通过 cyber.incidents@kyndryl.com 提供此类通知。供应商将提供 Kyndryl 合理请求的信息，包括有关此类安全违规的信息，以及供应商采取的任何补救和恢复活动的状态。合理请求的信息主要涉及安全违规情况或供应商所采取的补救和恢复活动，例如，用于表明针对设备、系统或应用的特权访问权限、管理员访问权限和其他访问权限的日志；设备、系统或应用的取证图像；以及其他事项。

2.4 供应商将向 Kyndryl 提供合理的协助，以履行与 Kyndryl、Kyndryl 关联公司和客户（及其客户和关联公司）有关安全违规的任何法律义务（包括通知监管机构或数据主体的义务）。

2.5 供应商不得通知或告知任何第三方安全违规直接或间接与 Kyndryl 或 Kyndryl 材料有关，除非 Kyndryl 书面批准或法律要求这样做。如果任何法律要求的通知将直接或间接地透露 Kyndryl 的身份，则供应商应在向任何第三方发布此类通知之前，以书面形式告知 Kyndryl。

2.6 如果由于供应商违反此类条款下的任何义务而导致安全违规：

(a) 供应商应负责支付 Kyndryl 在向适用的监管机构或其他政府部门及相关行业自我监管机构、向媒体（如果适用法律要求）、数据主体、客户和其他人通知安全违规时所产生的费用。

(b) 如果 Kyndryl 要求，供应商应自费建立并维护呼叫中心，以在将安全违规通知此类数据主体之日起一年内回答数据主体关于安全违规及其后果的问题，或遵循任何适用数据保护法的要求，以保护级别更高的方式为准。Kyndryl 和供应商应共同创建脚本和其他材料，以供呼叫中心人员在回复咨询时使用。或者，在书面通知供应商后，Kyndryl 可以建立并维护自己的呼叫中心，而不是让供应商建立呼叫中心，并且供应商应偿还 Kyndryl 在建立和维护此类呼叫中心时产生的实际费用，以及

(c) 供应商应在向受数据违规影响并选择注册此类服务的所有个人发出数据违规通知之日起的 1 年内，向 Kyndryl 偿付提供信用监控和信用恢复服务的实际费用，或遵循适用的任何数据保护法的要求，以保护级别更高的方式为准。

3. 物理安全和入口控制（以下所用的“设施”是指供应商托管、处理或以其他方式访问 Kyndryl 材料的物理位置）。

3.1 供应商应维护适当的物理进入控制，例如障碍、卡控入口点、监控摄像机和人控接待台，以防止未经授权进入设施的行为。

3.2 供应商将需要获得批准才能进入设施和设施内的受控区域（包括任何临时通道），并且将根据工作角色和业务需求来限制进入。如果供应商授予临时访问权限，则其授权员工应护送任何访问者进入设施和任何受控区域。

3.3 供应商应实施物理访问控制，包括多因素访问控制，这些控制与行业最佳实践相一致，以便适当地限制进入设备中的受控区域，供应商应记录所有进入尝试，并将此类日志保留至少一年。

3.4 供应商将在 (a) 授权的供应商员工离职后，或 (b) 授权的供应商员工不再具有有效的业务访问需求时，撤消对设施和设施内受控区域的访问权限。供应商应遵循正式记录在案的离职程序，包括立即将离职员工从访问控制列表中删除和退还实物门禁卡。

3.5 供应商应采取预防措施，保护用于支持服务和可交付成果以及 Kyndryl 技术处理的所有物理基础设施免遭自然和人为的环境威胁，例如环境温度过高、火灾、洪水、潮湿、盗窃和破坏行为。

4. 访问、干预、转移和分离控制

4.1 供应商将维护由供应商在其服务运营、提供可交付成果和 Kyndryl 技术处理期间所管理的记录在案的网络安全架构。供应商将分别审查此类网络体系结构，并采取措施防止未经授权的网络连接到系统、应用程序和网络设备，以遵守安全分段、隔离和深度防御标准。供应商不得在其任何托管服务的托管和运营中使用无线技术；除此之外，供应商可以在其服务和可交付成果的交付以及 Kyndryl 技术处理时使用无线网络技术，但供应商必须对任何此类无线网络进行加密并要求安全认证。

4.2 供应商应维护旨在从逻辑上分离任何 Kyndryl 材料并防止未经授权的人员接触或访问此类数据的措施。此外，供应商应对其生产环境、非生产环境和其他环境保持相应的隔离，并且如果 Kyndryl 材料已经存在于或被传输至非生产环境（例如为了重现错误），那么供应商应确保非生产环境内的安全和隐私保护措施等同于生产环境内的相应措施。

4.3 供应商应对传输中和静态的 Kyndryl 材料进行加密（除非供应商向 Kyndryl 合理地证明，对静态 Kyndryl 材料进行加密在技术上不可行）。供应商还将加密所有的物理介质（如果有），例如包含备份文件的介质。供应商应维护用于保护密钥生成、发布、分发、存储、轮换、撤销、恢复、备份、销毁、访问和数据加密相关使用的记录在案的程序。供应商应确保用于此类加密的特定加密方法符合行业最佳实践（例如 NIST SP 800-131a）。

4.4 如果供应商需要访问 Kyndryl 材料，那么供应商应将此类访问限制和限定到提供和支持此服务和可交付成果所需的最低级别。供应商应要求此类访问，包括对任何底层组件的管理访问（即特权访问），将是单独的、基于角色，并且需要经过供应商授权员工按照职责划分原则进行批准和定期验证。

供应商将采取措施来识别和删除多余和休眠的帐户。供应商还将在帐户所有者离职或 Kyndryl 或任何授权的供应商员工（例如帐户所有者的经理）提出要求后的二十四 (24) 小时内撤销具有特权访问权限的帐户。

4.5 与行业最佳实践相一致，供应商应维护实施停滞会话超时、多次连续登录尝试失败后帐户锁定、高强度密码或口令验证的技术措施，以及要求安全转移和存储此类密码和口令的措施。此外，供应商应对所有基于非控制台对任何 Kyndryl 材料的特权访问使用多因子身份认证。

4.6 供应商应监控特权访问权限的使用并维护安全信息和事件管理措施，这些措施旨在：(a) 识别未经授权的访问和活动，(b) 促进对于此类访问和活动的及时和适当的响应，以及 (c) 支持由供应商、Kyndryl（根据此类条款中的验证权利，以及交易文件和双方间的基本协议或其他相关协议中的审计权利）和其他人对记录在案的供应商策略的遵守情况进行审计。

4.7 供应商将保留日志，该日志记录了遵循行业最佳实践，对用于提供服务或可交付成果以及处理 Kyndryl 技术的系统的所有管理、用户或其他访问或活动（并在 Kyndryl 要求时向其提供这些日志）。供应商将维护旨在防止未经授权访问、修改和意外或故意破坏此类日志行为的措施。

4.8 供应商应保持对其拥有或管理的系统（包括最终用户系统）及其用于提供服务或可交付成果以及处理 Kyndryl 技术的系统的计算保护，此类保护包括：端点防火墙、全盘加密、用于解决恶意软件和高级持续性威胁的基于签名和非签名的端点检测和响应技术、基于时间的屏幕锁定，以及实施安全配置和修补需求的端点管理解决方案。此外，供应商应实施技术和操作控制，以确保仅允许已知且受信任的最终用户系统使用供应商网络。

4.9 根据行业最佳实践，供应商应对存在或处理 Kyndryl 材料的数据中心环境持续实施保护，包括：入侵检测和预防以及拒绝服务攻击的对策和缓解措施。

5. 服务及系统完整性和可用性控制

5.1 供应商应 (a) 至少每年执行一次安全性和隐私风险评估；(b) 正式版本发布之前和之后，针对服务和可交付成果以及 Kyndryl 技术处理，每年进行安全测试和漏洞评估，包括自动化系统和应用程序安全扫描和手动道德黑客攻击；(c) 征集一家合格的独立第三方来至少每年执行一次渗透测试，确保符合行业最佳实践，该类测试包括自动测试和手动测试；(d) 执行自动化管理和日常验证，以确保符合服务和可交付成果的每个组件以及 Kyndryl 技术处理的安全配置要求；以及 (e) 根据相关风险、可利用性和影响来修复已识别的漏洞或纠正不符合其安全配置要求的行为。在执行测试、评估、扫描以及修复活动时，供应商应采取合理步骤措施以避免服务中断。在 Kyndryl 要求时，供应商应向 Kyndryl 提供供应商当时最新的渗透测试活动的书面汇总，该报告应至少包含测试所涵盖的产品名称、测试范围内的系统或应用程序数量、测试日期、测试中使用的方法以及测试结果的高级汇总。

5.2 供应商将维护旨在管理对服务或可交付成果或 Kyndryl 技术处理应用变更相关风险的政策和程序。在实施此类变更（包括对受影响的系统、网络和基础组件的变更）之前，供应商应在已注册的变更请求中记录以下内容：(a) 变更的描述和变更原因；(b) 实施细节和安排；(c) 一份解释对服务和可交付成果、服务客户或 Kyndryl 材料的影响的风险声明；(d) 预期成果；(e) 回滚计划；以及 (f) 授权供应商员工的批准。

5.3 供应商应维护服务运营、提供可交付成果和 Kyndryl 技术处理中使用的所有 IT 资产库存。供应商将持续监视和管理此类 IT 资产、服务、可交付成果和 Kyndryl 技术的运行状况（包括容量）和可用性，包括此类资产、服务、可交付成果和 Kyndryl 技术的底层组件。

5.4 供应商应根据预定义的系统安全映像或安全基准来构建其在服务和可交付成果以及其 Kyndryl 技术处理的开发或运营中使用的所有系统，这些系统应符合行业最佳实践，例如互联网安全中心 (CIS) 基准。

5.5 在不限制供应商在交易文档或双方间相关基本协议下承担的义务或 Kyndryl 权利的前提下，对于业务连续性而言，供应商应根据记录在案的风险管理指南，对每项服务和可交付成果及处理 Kyndryl 技术所用的每个 IT 系统分别进行业务和 IT 连续性以及灾难恢复要求评估。在此类风险评估许可的范

围内，供应商应确保每项服务、可交付成果和 IT 系统具有与行业最佳实践相一致的独立定义、记录、维护以及每年验证的业务和 IT 连续性以及灾难恢复计划。供应商将确保此类计划旨在实现以下第 5.6 条中规定的特定恢复时间。

5.6 任何托管服务的特定恢复点目标 ("**RPO**") 和恢复时间目标 ("**RTO**") 均为：24 小时 RPO 和 24 小时 RTO；否则，在 Kyndryl 以书面形式通知供应商此类较短持续时间的 RPO 或 RTO（电子邮件构成书面内容）后，供应商应立即兑现 Kyndryl 已向客户承诺的任何较短持续时间的 RPO 或 RTO。由于涉及供应商向 Kyndryl 提供的所有其他服务，供应商应确保其业务连续性和灾难恢复计划旨在提供使供应商能够遵守其在交易文件和双方间的相关基本协议下对 Kyndryl 的所有义务的 RPO 和 RTO，包括供应商对及时提供测试、支持和维护的义务。

5.7 供应商应维护旨在对服务和可交付成果及相关系统、网络、应用程序以及这些服务和可交付成果范围内的底层组件进行评估、测试和应用安全咨询补丁的措施，以及用于处理 Kyndryl 技术的系统、网络、应用程序和底层组件的措施。在确定安全咨询补丁适用且适当的情况下，供应商应根据记录在案的严重性和风险评估准则实施补丁。供应商对安全咨询补丁的实施将遵循其自身的变更管理策略。

5.8 如果 Kyndryl 有合理的理由相信供应商提供给 Kyndryl 的硬件或软件可能包含侵入性元素，例如间谍软件、恶意软件或恶意代码，那么供应商需及时与 Kyndryl 合作，对 Kyndryl 的问题展开调查并采取补救措施。

6. 服务配置

6.1 供应商将支持对 Kyndryl 用户或客户帐户使用行业通用的联合身份验证方法，并且供应商将在遵循行业最佳实践的情况下对 Kyndryl 用户或客户帐户进行身份认证（例如，通过 Kyndryl 集中管理的多因子单点登录 (SSO)，使用 OpenID Connect 或安全性断言标记语言）。

7. 转包商。在不限制供应商在交易文档或双方间相关基本协议下承担的义务或 Kyndryl 权利的前提下，在保留转包商方面，供应商应确保为供应商执行工作的任何转包商均已实行监管控制措施，以遵循此类条款下供应商的要求和义务。

8. 物理介质。供应商将按照介质清理的行业最佳实践，在重用之前对将要重用的物理介质进行安全清理，并销毁不打算重用的物理介质。

第 IX 条，托管服务的认证和报告

如果供应商向 Kyndryl 提供托管服务，则本条款适用。

1.1 供应商应在以下规定的时间范围内获得下述认证或报告：

认证/报告	**时间范围**
关于供应商的托管服务： 符合以下标准的认证：ISO 27001、信息技术、安全技术、信息安全管理系统，此类认证由信誉良好的独立审核员评估得出 **或者** SOC 2 Type 2：由信誉良好的独立审计员提交的报告，证明其根据 SOC 2 Type 2 对供应商的系统、控制和操作进行了审查（至少包括安全性、隐私性和可用性）。	供应商应在本交易文件生效日期*或假定日期**后的 120 天内获得 ISO 27001 认证，然后由信誉良好的独立审核员评估，每 12 个月更新一次认证（每次更新均以当时最新版本的标准为准。） 供应商将在本交易文件生效日期*或假定日期**后的 240 天内获得 SOC 2 Type 2 报告，然后每 12 个月获取一次由信誉良好的独立审计员提交的一份新报告，证明其根据 SOC 2 Type 2 对供应商的系统、控制和操作进行了审查（至少包括安全性、隐私性和可用性） * 前提是，自生效日期起，供应商提供了托管服务 ** 供应商履行提供托管服务义务的日期

1.2 如果供应商提出书面要求，并且 Kyndryl 书面批准，则供应商可以获得与上述基本等同的证明或报告，且上表中所列的时间范围对于基本等同的证明或报告适用，无需任何更改。

1.3 供应商应：(a) 在 Kyndryl 要求时，立即向 Kyndryl 提供供应商有义务获取的每份认证和报告的副本，以及 (b) 及时解决 SOC 2 审查或基本等同（若 Kyndryl 批准）的审查中指出的任何内部控制弱点。

第X条，合作、认证和补救

如果供应商向 Kyndryl 提供任何服务或可交付成果，则本条款适用。

1. 供应商合作

1.1 如果 Kyndryl 有理由质疑任何服务或可交付成果是否可能会、正在或将要带来任何网络安全问题，那么供应商将与 Kyndryl 合作调查此类问题，包括及时、全面地响应信息请求，无论通过文件、其他记录还是相关供应商人员的采访等。

1.2 各方将同意：(a) 根据对方的要求提供进一步的信息，(b) 执行并相互交付此类其他文件，以及 (c) 在另一方合理请求时，执行此类其他操作和相关事宜，以达成此类条款以及此类条款中所引用文件的意图。例如，如果 Kyndryl 要求，供应商应及时提供与分包处理机构和转包商的书面合同中有关隐私与安全性的条款，若供应商拥有相应权利，也可以授予对合同的访问权。

1.3 如果 Kyndryl 要求，供应商将及时提供有关制造、开发或外包可交付成果及其组件的国家/地区的信息。

2. 验证（以下所用的“设施”是指供应商托管、处理或以其他方式访问 Kyndryl 材料的物理位置）

2.1 供应商将保留可审计的记录，以证明遵守这些条款。

2.2 Kyndryl 在提前 30 天书面通知供应商后，可自行或通过外部审核员验证供应商是否遵守这些条款，包括出于此目的访问任何设施，若无充分的理由相信访问供应商处理 Kyndryl 数据所在的任何数据中心可获得相关信息，那么 Kyndryl 将不会进行访问。供应商将与 Kyndryl 合作进行本次验证，包括及时、全面地响应信息请求，无论通过文件、其他记录还是相关供应商人员的采访等。供应商可以提供其遵守经批准的行为准则或行业认证的证明，或者以其他方式提供信息以证明遵守这些条款，以供 Kyndryl 考量。

2.3 在任意 12 个月内，最多进行一次验证，除非：(a) Kyndryl 正在验证供应商对 12 个月内先前验证中查出的问题所做的补救，或者 (b) 发生了安全违规，并且 Kyndryl 希望验证是否履行与此违规相关的义务。在这两种情况下，Kyndryl 都将按上述 2.2 条中的规定提前 30 天发出书面通知，但是要解决紧急的安全违规，Kyndryl 发出书面通知进行验证的提前时间可能不足 30 天。

2.4. 如 2.2 条和 2.3 条所规定，监管者和控制者可与 Kyndryl 享有相同权利，但监管者依照法律可能享有其他权利。

2.5 如果 Kyndryl 有合理依据得出供应商未遵守任何本条款的结论（无论该依据来自本条款项下的验证或其他），则供应商应立即纠正该等不合规行为。

3. 防伪计划

3.1 如果供应商的可交付成果包括电子元件（例如硬盘驱动器、固态驱动器、内存、中央处理器、逻辑设备或电缆），则供应商将维护并遵循书面的防伪计划，从而首先防止供应商向 Kyndryl 提供假冒元件，其次，在供应商不小心向 Kyndryl 提供假冒组件的情况下，立即进行检测并采取补救措施。供应商会让所有为 Kyndryl 提供电子元件的供应商（包括给 Kyndryl 提供可交付成果的供应商）承担同样的义务，以维护并遵循书面的防伪计划。

4. 补救

4.1 如果供应商因未能履行其在此类条款下的任何义务，导致安全违规，那么供应商将采取纠正行动，并补救该安全违规带来的有害影响，且此类行动和补救措施将按照 Kyndryl 的合理指示和安排进行。然而，如果安全违规是由供应商提供多租户托管服务引起的，并因此影响到包括 Kyndryl 在内的许多供应商客户，则鉴于安全违规的性质，供应商应及时适当地采取纠正行动，并补救该安全违规带来的有害影响，同时适当考虑 Kyndryl 对此类纠正和补救措施的任何意见。在不影响上述规定的情况下，如果供应商不能再遵守适用数据保护法律规定的义务，则供应商必须立即通知 Kyndryl。

4.2 Kyndryl 有权在其认为适当或必要的情况下，参与第 4.1 条中提及的任何安全违规的补救行动，供应商将负责纠正工作的成本和费用，以及双方因任何该等安全违规而产生的补救成本和费用。

4.3 举例来说，与安全违规相关的补救成本和费用可包括用于检测和调查安全违规、确定适用法律和法规下的责任、发出违规通知、建立和维护呼叫中心、提供信用监控和信用恢复服务、重新加载数据、纠正产品缺陷（包括通过源代码或其他开发方式）、保留第三方以协助前述或其他相关活动的相关成本和费用，以及补救安全违规所带来的有害影响所需的其他成本和费用。清楚起见，补救成本和费用不包括 Kyndryl 的利润损失、业务丢失、价值降低、收入降低、商誉受损或预期的成本节约。