Article I, Business Contact Information

This Article applies if Supplier or Kyndryl Processes the other's BCI.

1.1 Kyndryl and Supplier may Process the other's BCI wherever they do business in connection with Supplier's delivery of Services and Deliverables.

1.2 A party:

(a) will not use or disclose the other party's BCI for any other purpose (for clarity, neither party will Sell the other's BCI or use or disclose the other's BCI for any marketing purpose without the other party's prior written consent, and where required, the prior written consent of affected Data Subjects), and

(b) will delete, modify, correct, return, provide information about the Processing of, restrict the Processing of, or take any other reasonably requested action in respect of the other's BCI, promptly on written request from the other party.

1.3 The parties are not entering a joint Controller relationship regarding each other's BCI and no provision of the Transaction Document will be interpreted or construed as indicating any intent to establish a joint Controller relationship.

1.4 The Kyndryl Privacy Statement at https://www.kyndryl.com/privacy contains additional details on Kyndryl's Processing of BCI.

1.5 The parties have implemented and will maintain technical and organizational security measures to protect the other's BCI against loss, destruction, alteration, accidental or unauthorized disclosure, accidental or unauthorized access, and unlawful Processing.

Pasal I, Informasi Kontak Bisnis

Pasal ini berlaku jika Pemasok atau Kyndryl Memproses BCI lainnya.

1.1 Kyndryl dan Pemasok dapat Memproses BCI lain di mana pun mereka menjalankan bisnis berkaitan dengan penyampaian Layanan dan Materi yang Disampaikan oleh Pemasok.

1.2 Suatu pihak:

(a) tidak akan menggunakan atau mengungkapkan BCI pihak lain untuk tujuan apa pun lainnya (untuk kejelasan, tidak satu pun pihak akan Menjual BCI lain atau menggunakan atau mengungkapkan BCI lain untuk tujuan pemasaran apa pun tanpa persetujuan tertulis sebelumnya dari pihak lainnya, dan apabila diperlukan, persetujuan tertulis sebelumnya dari Subjek Data yang terpengaruh), dan

(b) akan menghapus, memodifikasi, mengoreksi, mengembalikan, memberikan informasi mengenai Pemrosesan, membatasi Pemrosesan, atau mengambil tindakan apa pun lainnya yang diminta secara wajar sehubungan dengan BCI lain, segera dengan permintaan tertulis dari pihak lain.

1.3 Para pihak tidak mengadakan hubungan Pengontrol bersama terkait BCI satu sama lain dan tidak ada ketentuan Dokumen Transaksi yang akan diinterpretasikan atau ditafsirkan sebagai indikasi maksud apa pun untuk membangun hubungan Pengontrol bersama.

1.4 Pernyataan Kerahasiaan Kyndryl di https://www.kyndryl.com/privacy berisi rincian tambahan mengenai Pemrosesan BCI Kyndryl.

1.5 Para pihak telah mengimplementasikan dan akan memelihara tindakan keamanan teknis dan organisasi untuk melindungi BCI pihak lainnya terhadap kerugian, kerusakan, perubahan, pengungkapan secara tidak sengaja atau tidak sah, akses secara tidak sengaja atau tidak sah, dan Pemrosesan yang melanggar hukum.

1.6 Supplier will promptly (and in no event any later than 48 hours) notify Kyndryl after becoming aware of any Security Breach involving Kyndryl's BCI. Supplier will provide such notification to cyber.incidents@kyndryl.com. Supplier will provide Kyndryl with reasonably requested information about such breach and the status of any Supplier remediation and restoration activities. By way of example, reasonably requested information may include logs demonstrating privileged, administrative, and other access to Devices, systems or applications, forensic images of Devices, systems or applications, and other similar items, to the extent relevant to the breach or Supplier's remediation and restoration activities.

1.6 Pemasok akan segera (dan tidak lebih dari 48 jam) memberi tahu Kyndryl setelah mengetahui adanya Pelanggaran Keamanan yang melibatkan BCI Kyndryl. Pemasok akan memberikan pemberitahuan seperti ke cyber.incidents@kyndryl.com. Pemasok akan memberikan informasi yang diminta secara wajar kepada Kyndryl mengenai pelanggaran tersebut dan status setiap aktivitas perbaikan dan restorasi Pemasok. Sebagai contoh, informasi yang diminta secara wajar dapat mencakup log yang mendemonstrasikan akses istimewa, administratif, dan akses lain ke Perangkat, sistem atau aplikasi, gambar forensik Perangkat, sistem atau aplikasi, dan item serupa lainnya, sejauh relevan dengan pelanggaran atau aktivitas perbaikan dan restorasi Pemasok.

1.7 Where Supplier is only Processing Kyndryl's BCI, and has no access to any other data or materials of any kind or to any Kyndryl Corporate System, this Article and Article X (Cooperation, Verification and Remediation) are the only Articles that apply to such Processing.

1.7 Di mana Pemasok hanya Memproses BCI Kyndryl, dan tidak memiliki akses ke data atau materi apa pun lainnya dalam bentuk apa pun atau ke setiap Sistem Korporasi Kyndryl, Pasal ini dan Pasal X (Kerja Sama, Verifikasi, dan Remediasi) adalah satu-satunya Pasal yang berlaku untuk Pemrosesan tersebut.

Article II, Technical and Organizational Measures, Data Security

This Article applies if Supplier Processes Kyndryl Data, other than Kyndryl's BCI. Supplier will comply with the requirements of this Article in providing all Services and Deliverables, and by doing so protect Kyndryl Data against loss, destruction, alteration, accidental or unauthorized disclosure, accidental or unauthorized access, and unlawful forms of Processing. The requirements of this Article extend to all IT applications, platforms, and infrastructure that Supplier operates or manages in providing Deliverables and Services, including all development, testing, hosting, support, operations, and data center environments.

1. Data Use

1.1 Supplier may not add to the Kyndryl Data or include with the Kyndryl Data any other information or data, including any Personal Data, without Kyndryl's prior written consent, and Supplier may not use Kyndryl Data in any form, aggregated or otherwise, for any purpose other than providing Services and Deliverables (by way of example, Supplier is not permitted to use or reuse Kyndryl Data to evaluate the effectiveness of or means of improving Supplier's offerings, for research and development to create new offerings, or to generate reports regarding Supplier's offerings). Unless expressly permitted in the Transaction Document, Supplier is prohibited from Selling Kyndryl Data.

1.2 Supplier will not embed any web tracking technologies in the Deliverables or as part of the Services (such technologies include HTML5, local storage, third party tags or tokens, and web beacons) unless expressly permitted in the Transaction Document.

2. Third Party Requests and Confidentiality

2.1 Supplier will not disclose Kyndryl Data to any third party, unless authorized in advance by Kyndryl in writing. If a government, including any regulator, demands access to Kyndryl Data (e.g., if

Pasal II, Tindakan Teknis dan Organisasi, Keamanan Data

Pasal ini berlaku jika Pemasok Memproses Data Kyndryl, selain BCI Kyndryl. Pemasok akan mematuhi persyaratan Pasal ini dalam memberikan semua Layanan dan Materi yang Disampaikan, dan sekaligus melindungi Data Kyndryl terhadap kerugian, kerusakan, perubahan, pengungkapan secara tidak sengaja atau tidak sah, akses secara tidak sengaja atau tidak sah, dan bentuk Pemrosesan yang melanggar hukum. Persyaratan Pasal ini menjangkau semua aplikasi, platform, dan infrastruktur TI yang mana dan yang dioperasikan atau dikelola oleh Pemasok dalam memberikan Materi yang Disampaikan dan Layanan, termasuk semua pengembangan, pengujian, hosting, dukungan, operasi, dan lingkungan pusat data.

1. Penggunaan Data

1.1 Pemasok tidak dapat menambahkan setiap informasi atau data lain, termasuk setiap Data Pribadi, tanpa persetujuan tertulis sebelumnya dari Kyndryl ke Data Kyndryl atau menyertakan dengan Data Kyndryl, dan Pemasok tidak dapat menggunakan Data Kyndryl dalam bentuk apa pun, secara agregat atau sebaliknya, untuk tujuan apa pun selain memberikan Layanan dan Materi yang Disampaikan (sebagai contoh, Pemasok tidak diizinkan untuk menggunakan atau menggunakan kembali Data Kyndryl untuk mengevaluasi efektivitas atau sarana untuk meningkatkan tawaran Pemasok, untuk penelitian dan pengembangan guna membuat tawaran baru, atau untuk menghasilkan laporan terkait tawaran Pemasok). Kecuali apabila diizinkan dalam Dokumen Transaksi, Pemasok dilarang Menjual Data Kyndryl.

1.2 Pemasok tidak akan menyematkan setiap teknologi pelacakan web dalam Materi yang Disampaikan atau sebagai bagian dari Layanan (teknologi tersebut mencakup HTML5, penyimpanan lokal, tag atau token pihak ketiga, dan web beacon) kecuali apabila secara tegas diizinkan dalam Dokumen Transaksi.

2. Kerahasiaan dan Permintaan Pihak Ketiga

2.1 Pemasok tidak akan mengungkap Data Kyndryl kepada pihak ketiga mana pun, kecuali apabila diberi wewenang sebelumnya oleh Kyndryl secara tertulis. Jika pemerintah, termasuk setiap

the U.S. government serves a national security order on Supplier to obtain Kyndryl Data), or if a disclosure of Kyndryl Data is otherwise required by law, Supplier will notify Kyndryl in writing of such demand or requirement and afford Kyndryl a reasonable opportunity to challenge any disclosure (where law prohibits notification, Supplier will take the steps that it reasonably believes are appropriate to challenge the prohibition and disclosure of Kyndryl Data through judicial action or other means).

2.2 Supplier assures Kyndryl that: (a) only those of its employees who need access to Kyndryl Data to provide Services or Deliverables will have that access, and then only to the extent necessary to provide those Services and Deliverables; and (b) it has bound its employees to confidentiality obligations that require those employees to only use and disclose Kyndryl Data as these Terms permit.

3. **Return or Deletion of Kyndryl Data**

3.1 Supplier will, at Kyndryl's choice, either delete or return Kyndryl Data to Kyndryl upon termination or expiration of the Transaction Document, or earlier upon request from Kyndryl. If Kyndryl requires deletion, then Supplier will, consistent with Industry Best Practices, render the data unreadable and unable to be reassembled or reconstructed, and will certify the deletion to Kyndryl. If Kyndryl requires the return of Kyndryl Data, then Supplier will do so on Kyndryl's reasonable schedule and per Kyndryl's reasonable written instructions.

pembuat peraturan, meminta akses ke Data Kyndryl (misalnya, jika pemerintah AS menyerahkan pemberitahuan ketertiban keamanan nasional kepada Pemasok untuk memperoleh Data Kyndryl), atau jika pengungkapan Data Kyndryl diwajibkan oleh hukum, Pemasok akan memberi tahu Kyndryl secara tertulis mengenai permintaan atau persyaratan tersebut dan memberi Kyndryl peluang yang wajar untuk berkeberatan dengan pengungkapan apa pun (jika hukum melarang pemberitahuan, Pemasok akan mengambil langkah yang diyakini secara wajar sesuai untuk berkeberatan dengan pelarangan dan pengungkapan Data Kyndryl melalui tindakan yudisial atau cara lainnya).

2.2 Pemasok memastikan Kyndryl bahwa: (a) hanya karyawan yang perlu akses ke Data Kyndryl untuk memberikan Layanan atau Materi yang Disampaikan yang akan memiliki akses, dan kemudian hanya sejauh diperlukan untuk memberikan Layanan dan Materi yang Disampaikan tersebut; dan (b) Pemasok telah mengikat karyawannya pada kewajiban kerahasiaan yang mensyaratkan karyawan tersebut untuk hanya menggunakan dan mengungkapkan Data Kyndryl sebagaimana yang diizinkan dalam Syarat-Syarat ini.

3. **Pengembalian atau Penghapusan Data Kyndryl**

3.1 Pemasok akan, atas pilihan Kyndryl, menghapus atau mengembalikan Data Kyndryl kepada Kyndryl setelah pengakhiran atau habis masa berlaku Dokumen Transaksi, atau lebih awal atas permintaan dari Kyndryl. Jika Kyndryl mensyaratkan penghapusan, Pemasok akan, sesuai dengan Praktik Terbaik Industri, menyajikan data yang tidak dapat dibaca dan tidak dapat disusun ulang atau direkonstruksi, dan akan menjamin penghapusan ke Kyndryl. Jika Kyndryl mewajibkan pengembalian Data Kyndryl, Pemasok akan melakukannya pada jadwal Kyndryl yang wajar dan sesuai dengan instruksi tertulis Kyndryl yang wajar.

Article III, Privacy

This Article applies if Supplier Processes Kyndryl Personal Data.

1. Processing

1.1 Kyndryl appoints Supplier as a Processor to Process Kyndryl Personal Data for the sole purpose of providing the Deliverables and Services in accordance with Kyndryl's instructions, including those contained in these Terms, the Transaction Document and the associated base agreement between the parties. If Supplier does not accommodate an instruction, Kyndryl may terminate the affected part of the Services on written notice. If Supplier believes an instruction violates a data protection law, Supplier will so inform Kyndryl promptly and within any time frame required by the law.

1.2 Supplier will comply with all data protection laws applicable to the Services and Deliverables.

1.3 An Exhibit to the Transaction Document, or the Transaction Document itself, sets out the following in respect of Kyndryl Data:

(a) categories of Data Subjects;
(b) types of Kyndryl Personal Data;
(c) data actions and Processing activities;
(d) duration and frequency of Processing; and
(e) a list of Subprocessors.

2. Technical and Organizational Measures

2.1 Supplier will implement and maintain the technical and organizational measures set forth in Article II (Technical and Organizational Measures, Data Security) and Article VIII (Technical and Organizational Measures, General Security), and by doing so ensure a level of security appropriate to the risk its Services and Deliverables present. Supplier certifies and understands the restrictions in Article II, this Article III, and Article VIII and will comply with them.

3. Data Subject Rights and Requests

3.1 Supplier will inform Kyndryl promptly (on a schedule that allows Kyndryl and any Other

Pasal III, Kerahasiaan

Pasal ini berlaku jika Pemasok Memproses Data Pribadi Kyndryl.

1. Pemrosesan

1.1 Kyndryl menunjuk Pemasok sebagai Prosesor untuk Memproses Data Pribadi Kyndryl semata untuk tujuan memberikan Materi yang Disampaikan dan Layanan sesuai dengan instruksi Kyndryl, termasuk yang termuat dalam Syarat-Syarat ini, Dokumen Transaksi, dan perjanjian dasar terkait di antara para pihak. Jika Pemasok tidak mengakomodasi instruksi, Kyndryl dapat mengakhiri bagian Layanan yang terdampak dengan pemberitahuan tertulis. Apabila Pemasok meyakini bahwa suatu instruksi melanggar hukum perlindungan data, Pemasok akan segera menginformasikan kepada Kyndryl dan dalam kerangka waktu kapan pun yang diwajibkan oleh hukum.

1.2 Pemasok akan mematuhi semua peraturan perundang-undangan perlindungan data yang berlaku untuk Layanan dan Materi yang Disampaikan.

1.3 Ekshibit untuk Dokumen Transaksi, atau Dokumen Transaksi itu sendiri, menjabarkan hal-hal berikut berkenaan dengan Data Kyndryl:

(a) kategori Subjek Data;
(b) jenis Data Pribadi Kyndryl;
(c) tindakan data dan aktivitas Pemrosesan;
(d) durasi dan frekuensi Pemrosesan; dan
(e) daftar Subprosesor.

2. Tindakan Teknis dan Organisasi

2.1 Pemasok akan mengimplementasikan dan mempertahankan tindakan teknis dan organisasi yang dijabarkan dalam Pasal II (Tindakan Teknis dan Organisasi, Keamanan Data) dan Pasal VIII (Tindakan Teknis dan Organisasi, Keamanan Umum), dan sekaligus memastikan tingkat keamanan yang sesuai untuk risiko yang diberikan Layanan dan Materi yang Disampaikan. Pemasok menyatakan dan memahami bahwa pembatasan dalam Pasal II, Pasal III ini, dan Pasal VIII dan akan mematuhinya.

3. Permintaan dan Hak Subjek Data

3.1 Pemasok akan segera menginformasikan kepada Kyndryl (pada jadwal yang mengizinkan

Controllers to fulfill their legal obligations) of any request from a Data Subject to exercise any Data Subject rights (e.g., rectification, deletion or blocking of data) regarding Kyndryl Personal Data. Supplier may also promptly direct a Data Subject making such a request to Kyndryl. Supplier will not answer any requests from Data Subjects unless it is legally required or instructed by Kyndryl in writing to do so.

Kyndryl dan setiap Pengontrol lainnya untuk memenuhi kewajiban hukum mereka) mengenai setiap permintaan dari Subjek Data untuk melaksanakan setiap hak Subjek Data (misalnya, pembetulan, penghapusan, atau pemblokiran data) terkait Data Pribadi Kyndryl. Pemasok juga dapat segera mengarahkan Subjek Data yang mengajukan permintaan tersebut kepada Kyndryl. Pemasok tidak akan memberikan jawaban atas permintaan apa pun dari Subjek Data kecuali diwajibkan secara hukum atau diinstruksikan secara tertulis oleh Kyndryl untuk melakukan hal tersebut.

3.2 If Kyndryl is obliged to provide information regarding Kyndryl Personal Data to Other Controllers or other third-parties (e.g., Data Subjects or regulators), Supplier will assist Kyndryl by providing information and taking other reasonable actions that Kyndryl requests, on a schedule that allows Kyndryl to timely respond to such Other Controllers or third-parties.

3.2 Apabila Kyndryl berkewajiban untuk memberikan informasi mengenai Data Pribadi Kyndryl kepada Pengontrol Lain atau pihak ketiga lainnya (misalnya Subjek Data atau pembuat peraturan), Pemasok akan membantu Kyndryl dengan memberikan informasi dan mengambil tindakan lain yang wajar sebagaimana yang diminta oleh Kyndryl, pada jadwal yang mengizinkan Kyndryl untuk menanggapi secara tepat waktu ke Pengontrol Lain atau pihak ketiga tersebut.

4. Subprocessors

4. Subprosesor

4.1 Supplier will provide Kyndryl with advance written notice before adding a new Subprocessor or expanding the scope of Processing by an existing Subprocessor, with such written notice identifying the name of the Subprocessor and describing the new or expanded scope of Processing. Kyndryl may object to any such new Subprocessor or expanded scope on reasonable grounds at any time, and if it does so, the parties will work together in good faith to address Kyndryl's objection. Subject to Kyndryl's right to so object at any time, Supplier may commission the new Subprocessor or expand the scope of Processing of the existing Subprocessor if Kyndryl has not raised an objection within 30 Days of the date of Supplier's written notice.

4.1 Pemasok sebelumnya akan memberikan Kyndryl pemberitahuan tertulis sebelum menambahkan Subprosesor baru atau memperluas cakupan Pemrosesan oleh Subprosesor yang sudah ada, dengan pemberitahuan tertulis tersebut yang mengidentifikasi nama Subprosesor dan menguraikan cakupan yang baru atau diperluas dari Pemrosesan. Kyndryl dapat berkeberatan dengan setiap Subprosesor baru tersebut atau cakupan yang diperluas dengan landasan yang wajar kapan pun, dan jika demikian, para pihak akan bekerja bersama dengan iktikad baik untuk mengatasi keberatan Kyndryl. Dengan tunduk pada hak Kyndryl untuk berkeberatan kapan saja, Pemasok dapat memberi kuasa pada Subprosesor baru atau memperluas cakupan Pemrosesan Subprosesor yang sudah ada jika Kyndryl tidak mengajukan keberatan dalam waktu 30 Hari sejak tanggal pemberitahuan tertulis Pemasok.

4.2 Supplier will impose the data protection, security and certification obligations set out in these Terms on each approved Subprocessor prior to a Subprocessor Processing any Kyndryl Data. Supplier is fully liable to Kyndryl for performance of each Subprocessor's obligations.

4.2 Pemasok akan memikulkan kewajiban perlindungan data, keamanan, dan sertifikasi yang dijabarkan dalam Syarat-Syarat ini pada masing-masing Subprosesor yang disetujui sebelum Subprosesor Memproses setiap Data Kyndryl. Pemasok sepenuhnya bertanggung jawab kepada

Kyndryl atas kinerja masing-masing kewajiban Subprosesor.

5. Transborder Data Processing

As used below:

Adequate Country means a country providing an adequate level of data protection with respect to the relevant transfer pursuant to the applicable data protection laws or decisions of regulators.

Data Importer means either a Processor or a Subprocessor that is not established in an Adequate Country.

EU Standard Contractual Clauses ("EU SCCs") means the EU Standard Contractual Clauses (Commission Decision 2021/914) with optional clauses applied except for option 1 of Clause 9(a) and option 2 of Clause 17, as officially published at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Serbian Standard Contractual Clauses ("Serbian SCCs") means the Serbian Standard Contractual Clauses as adopted by the "Serbian Commissioner for Information of Public Importance and Personal Data Protection", published at https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Standard Contractual Clauses ("**SCCs**") means the contractual clauses required by applicable data protection laws for the transfer of Personal Data to Processors that are not established in Adequate Countries.

United Kingdom Standard Contractual Clauses ("UK SCCs") means the UK Standard Contractual Clauses for Controllers to Processors as officially published at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-

5. Pemrosesan Data Lintas Negara

Sebagaimana yang digunakan di bawah ini:

Negara yang Memadai berarti negara yang memberikan tingkat perlindungan data yang memadai sehubungan dengan transfer yang relevan menurut peraturan perundang-undangan perlindungan data yang berlaku atau keputusan pembuat peraturan.

Pengimpor Data berarti Prosesor atau Subprosesor yang tidak didirikan dalam suatu Negara yang Memadai.

Klausul Kontrak Standar EU (EU Standard Contractual Clauses - "EU SCC") berarti Klausul Kontrak Standar EU (Keputusan Komisi 2021/914) dengan klausul opsional yang diterapkan kecuali untuk opsi 1 Klausul 9(a) dan opsi 2 Klausul 17, sebagaimana yang dipublikasikan secara resmi di https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Klausul Kontrak Standar Serbia (Serbian Standard Contractual Clauses - "Serbian SCC") berarti Klausul Kontrak Standar Serbia sebagaimana yang diadopsi oleh "Komisioner Serbia untuk Informasi Kepentingan Publik dan Perlindungan Data Pribadi", yang dipublikasikan di https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx.

Klausul Kontrak Standar (Standard Contractual Clauses - "**SCC**") berarti klausul kontrak yang diwajibkan oleh peraturan perundang-undangan perlindungan data yang berlaku untuk transfer Data Pribadi ke Prosesor yang tidak didirikan dalam Negara yang Memadai.

Adendum Transfer Data Internasional Inggris untuk Klausul Kontrak Standar Komisi Uni Eropa ("Adendum Inggris") berarti Adendum Transfer Data Internasional Inggris untuk Klausul Kontrak Standar Komisi Uni Eropa sebagaimana yang dipublikasikan secara resmi di https://ico.org.uk/for-organisations/guide-to-data-

gdpr/international-transfers-after-uk-exit/sccs-after-transition-period/.

protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/

Swiss Addendum to the EU Commission Standard Contractual Clauses ("Swiss Addendum") means the contractual clauses to the EU Commission Standard Contractual Clauses which apply in accordance the decision of the Swiss Data Protection Authority (**"FDPIC"**) and in compliance with the Swiss Federal Act on Data Protection (**"FADP"**).

Adendum Swiss untuk Klausul Kontrak Standar Komisi UE ("Adendum Swiss") berarti klausul kontraktual untuk Klausul Kontrak Standar Komisi UE yang berlaku sesuai dengan keputusan Otoritas Perlindungan Data Swiss (**"FDPIC"**) dan sesuai dengan Undang-Undang Federal Swiss tentang Perlindungan Data (**"FADP"**).

5.1 Supplier will not transfer or disclose (including by remote access) any Kyndryl Personal Data across borders without Kyndryl's prior written consent. If Kyndryl provides such consent, the parties will cooperate to ensure compliance with applicable data protection laws. If SCCs are required by those laws, Supplier will promptly enter into the SCCs upon Kyndryl's request.

5.1 Pemasok tidak akan mentransfer atau mengungkap (termasuk dengan akses jarak jauh) setiap Data Pribadi Kyndryl lintas batas tanpa persetujuan tertulis dari Kyndryl sebelumnya. Jika Kyndryl memberikan persetujuan tersebut, para pihak akan bekerja sama guna memastikan kepatuhan dengan peraturan perundang-undangan perlindungan data yang berlaku. Jika SCC diwajibkan oleh peraturan perundang-undangan tersebut, Pemasok akan segera menandatangani SCC atas permintaan Kyndryl.

5.2 Regarding EU SCCs:

5.2 Mengenai SCC UE:

(a) If Supplier is not established in an Adequate Country: Supplier is hereby entering into EU SCCs as a Data Importer with Kyndryl, and Supplier will enter into written agreements with each approved Subprocessor, in accordance with Clause 9 of the EU SCCs, and will provide Kyndryl with copies of those agreements upon request.

(a) Apabila Pemasok tidak didirikan di Negara yang Memadai: Pemasok dengan ini menandatangani EU SCC sebagai Pengimpor Data dengan Kyndryl, dan Pemasok akan menandatangani perjanjian tertulis dengan masing-masing Subprosesor yang disetujui, sesuai dengan Klausul 9 EU SCC, dan akan memberikan salinan perjanjian tersebut kepada Kyndryl berdasarkan permintaan.

(i) Module 1 of the EU SCCs does not apply unless otherwise agreed by the parties in writing.

(i) Modul 1 EU SCC tidak berlaku kecuali jika disepakati lain oleh para pihak secara tertulis.

(ii) Module 2 of the EU SCCs applies where Kyndryl is a Controller and Module 3 applies where Kyndryl is a Processor. In accordance with Clause 13 of the EU SCCs, when Modules 2 or 3 apply, the parties agree that (1) the EU SCCs will be governed by the law of the EU member state where the competent supervisory authority is located and (2) any disputes arising from the EU SCCs will be in the courts of the EU member state where the competent supervisory authority is located. If such law in (1) does not allow for third-party beneficiary rights, then the EU SCCs

(ii) Modul 2 EU SCC berlaku jika Kyndryl adalah Pengontrol dan Modul 3 berlaku jika Kyndryl adalah Prosesor. Sesuai dengan Klausul 13 EU SCC, jika Modul 2 atau 3 berlaku, para pihak setuju bahwa (1) EU SCC akan diatur oleh hukum dari negara bagian anggota UE di mana otoritas pengawas yang kompeten berada dan (2) sengketa apa pun yang timbul dari EU SCC akan diselesaikan di pengadilan negara bagian anggota UE di mana otoritas pengawas yang kompeten berada. Apabila hukum tersebut dalam (1) tidak mengizinkan

shall be governed by the law of the Netherlands and any disputes arising from the EU SCCs under (2) shall be resolved by the court of Amsterdam in the Netherlands.

hak-hak penerima manfaat pihak ketiga, maka EU SCC akan diatur oleh hukum Belanda dan setiap sengketa yang timbul dari EU SCC berdasarkan (2) akan diselesaikan oleh pengadilan Amsterdam di Belanda.

(b) If Supplier is established in the European Economic Area and Kyndryl is a Controller not subject to the General Data Protection Regulation 2016/679, then Module 4 of the EU SCCs applies, and Supplier is hereby entering into EU SCCs as a data exporter with Kyndryl. If Module 4 of the EU SCCs applies, the parties agree that the EU SCCs shall be governed by the law of the Netherlands and any disputes arising from the EU SCCs shall be resolved by the court of Amsterdam in the Netherlands.

(b) Apabila Pemasok didirikan dalam Wilayah Ekonomi Eropa dan Kyndryl adalah Pengontrol yang tidak tunduk pada Peraturan Perlindungan Data Umum 2016/679, maka Modul 4 EU SCC akan berlaku, dan Pemasok dengan ini menandatangani EU SCC sebagai pengekspor data dengan Kyndryl. Apabila Modul 4 EU SCC berlaku, maka para pihak setuju bahwa EU SCC akan diatur oleh hukum Belanda dan setiap sengketa yang timbul dari EU SCC akan diselesaikan oleh pengadilan Amsterdam di Belanda.

(c) If Other Controllers, such as Customers or affiliates, request to become a party to EU SCCs pursuant to the ‘docking clause’ in Clause 7, Supplier hereby agrees to any such request.

(c) Apabila Pengontrol Lain, seperti Pelanggan atau afiliasi, meminta untuk menjadi pihak pada EU SCC sesuai dengan 'klausul docking' pada Klausul 7, Pemasok dengan ini menyetujui setiap permintaan tersebut.

(d) Technical and Organizational Measures required to complete Annex II of the EU SCCs can be found in these Terms, the Transaction Document itself, and the associated base agreement between the parties.

(d) Tindakan Teknis dan Organisasi yang diperlukan untuk melengkapi Aneks II EU SCC dapat ditemukan dalam Syarat-Syarat ini, Dokumen Transaksi itu sendiri, dan perjanjian dasar terkait antara para pihak.

(e) In the event of any conflict between the EU SCCs and these Terms, the EU SCCs will prevail.

(e) Apabila terdapat ketidaksesuaian apa pun antara EU SCC dan Syarat-Syarat ini, maka EU SCC yang akan berlaku.

5.3 Regarding UK Addendum(s):

5.3 Mengenai Adendum Inggris:

(a) If Supplier is not established in an Adequate Country: (i) Supplier is hereby entering into UK Addendum(s) with Kyndryl as an Importer to append to the EU SCCs set out above (as applicable, depending on the circumstances of the processing activities); and (ii) Supplier will enter into written agreements with each approved Subprocessor , and will provide Kyndryl with copies of those agreements upon request.

a) Jika Pemasok tidak didirikan di Negara Adekuat: (i) Pemasok dengan ini menandatangani Adendum Inggris dengan Kyndryl sebagai Importir untuk menambahkan EU SCC yang ditetapkan di atas (sebagaimana yang berlaku, tergantung pada keadaan terkait aktivitas pemrosesan); dan (ii) Pemasok akan mengadakan perjanjian tertulis dengan setiap Subprosesor yang disetujui, dan akan memberi Kyndryl salinan perjanjian tersebut jika diminta.

(b) If Supplier is established in an Adequate Country, and Kyndryl is a Controller not subject to the UK General Data Protection Regulation (as incorporated into UK law under the European Union (Withdrawal) Act 2018), then Supplier is hereby entering into UK Addendum(s) as an Exporter with

b) Jika Pemasok didirikan di Negara Adekuat, dan Kyndryl adalah Pengendali yang tidak tunduk pada Peraturan Perlindungan Data

Kyndryl to append to the EU SCCs set out in Section 5.2(b) above.

(c) If Other Controllers, such as Customers or affiliates, request to become a party to UK Addendum(s), Supplier hereby agrees to any such request.

(d) Appendix Information (as set out in Table 3) in the UK Addendum(s) can be found in the applicable EU SCCs, these Terms, the Transaction Document itself, and the associated base agreement between the parties. Neither Kyndryl nor Supplier can end the UK Addendum(s) when the UK Addendum changes.

(e) In the event of any conflict between the UK Addendum(s) and these Terms, the UK Addendum(s) will prevail.

Umum Inggris (sebagaimana yang digabungkan ke dalam hukum Inggris berdasarkan Undang-Undang Uni Eropa (Penarikan) 2018), maka Pemasok dengan ini menandatangani Adendum Inggris sebagai Eksportir dengan Kyndryl untuk ditambahkan ke EU SCC yang ditetapkan dalam Pasal 5.2(b) di atas.

c) Jika Pengendali Lain, seperti Pelanggan atau afiliasi, meminta untuk menjadi pihak dalam Adendum Inggris, Pemasok dengan ini menyetujui permintaan tersebut.

d) Informasi Apendiks (sebagaimana yang ditetapkan dalam Tabel 3) di Adendum Inggris dapat ditemukan di EU SCC yang berlaku, Syarat-Syarat ini, Dokumen Transaksi itu sendiri, serta perjanjian dasar terkait di antara para pihak. Baik Kyndryl maupun Pemasok tidak dapat mengakhiri Adendum Inggris apabila Adendum Inggris mengalami perubahan.

e) Apabila terjadi pertentangan antara Adendum Inggris dan Syarat-Syarat ini, Adendum Inggris akan diutamakan.

5.4 Regarding Serbian SCCs:

(a) If Supplier is not established in an Adequate Country: (i) Supplier is hereby entering into Serbian SCCs with Kyndryl on Supplier's own behalf as a Processor; and (ii) Supplier will enter into written agreements with each approved Subprocessor, in accordance with Article 8 of the Serbian SCCs, and will provide Kyndryl with copies of those agreements upon request.

(b) If Supplier is established in an Adequate Country, then Supplier is hereby entering into Serbian SCCs with Kyndryl on behalf of each Subprocessor located in a non-Adequate Country. If Supplier is unable to do so for any such Subprocessor, then Supplier will provide Kyndryl with the Serbian SCCs signed by that Subprocessor for Kyndryl's countersignature prior to allowing the Subprocessor to Process any Kyndryl Personal Data.

5.4 Perihal Serbian SCC:

(a) Apabila Pemasok tidak didirikan di Negara yang Memadai: (i) Pemasok dengan ini menandatangani Serbian SCC dengan Kyndryl atas nama Pemasok sendiri sebagai Prosesor; dan (ii) Pemasok akan menandatangani perjanjian tertulis dengan masing-masing Subprosesor yang disetujui, sesuai dengan Pasal 8 Serbian SCC, dan akan memberikan salinan perjanjian tersebut kepada Kyndryl berdasarkan permintaan.

(b) Apabila Pemasok didirikan di Negara yang Memadai, maka Pemasok dengan ini menandatangani Serbian SCC dengan Kyndryl atas nama masing-masing Subprosesor yang berada di Negara yang Tidak Memadai. Apabila Pemasok tidak dapat melakukannya untuk setiap Subprosesor tersebut, maka Pemasok akan memberikan Serbian SCC yang ditandatangani oleh Subprosesor tersebut kepada Kyndryl agar Kyndryl turut menandatangani sebelum mengizinkan Subprosesor untuk Memproses setiap Data Pribadi Kyndryl.

(c) The Serbian SCCs between Kyndryl and Supplier will serve either as Serbian SCCs between a Controller and Processor or as a back-to-back written agreement between 'processor' and 'sub-processor', as the facts require. In the event of any conflict between the Serbian SCCs and these Terms, the Serbian SCCs will prevail.

(c) Serbian SCC antara Kyndryl dan Pemasok akan berfungsi sebagai Serbian SCC antara Pengontrol dan Prosesor atau sebagai perjanjian tertulis konsekutif antara 'prosesor' dan 'subprosesor', sebagaimana yang dibutuhkan oleh fakta. Apabila terdapat ketidaksesuaian antara Serbian SCC dan Syarat-Syarat ini, maka Serbian SCC yang akan berlaku.

(d) Information required to complete Appendices 1 to 8 of the Serbian SCCs for the purpose of governing the transfer of Personal Data to a non-Adequate Country can be found in these Terms and in the Exhibit to the Transaction Document, or the Transaction Document itself.

(d) Informasi yang diperlukan untuk melengkapi Apendiks 1 hingga 8 dari Serbian SCC untuk tujuan mengatur transfer Data Pribadi ke Negara yang Tidak Memadai dapat ditemukan di Syarat-Syarat ini dan Ekshibit pada Dokumen Transaksi atau Dokumen Transaksi itu sendiri.

5.5. Regarding Swiss Addendum(s):

5.5. Mengenai Adendum Swiss:

(a) If and to the extent a transfer of Kyndryl Personal Data under section 5.1. is subject to the Swiss Federal Act on Data Protection ("FADP") the EU SCCs agreed in Section 5.2. of these Terms shall govern the transfer, with the following amendments to adopt the GDPR standard for Swiss Personal Data:

- References to the General Data Protection Regulation ("GDPR") shall be understood also as references to the equivalent provisions of the FADP,
- the Swiss Federal Data Protection Information Commission is the competent supervisory authority as per Clause 13 and Annex I.C of EU SCCs
- Swiss law as the governing law in case the transfer is exclusively subject to the FADP and
- The term "member state" in Clause 18 of the EU SCC shall be extended to include Switzerland for the purpose of allowing Swiss data subjects to pursue their rights in their place of habitual residence.

(a) Jika dan sejauh transfer Data Pribadi Kyndryl berdasarkan pasal 5.1. tunduk pada Undang-Undang Federal Swiss tentang Perlindungan Data ("FADP") EU SCC yang disetujui di Bagian 5.2. Syarat-Syarat ini akan mengatur transfer, dengan amendemen berikut untuk mengadopsi standar GDPR tentang Data Pribadi Swiss:

- Referensi Peraturan Perlindungan Data Umum ("GDPR") harus dipahami juga sebagai referensi untuk ketentuan yang setara dari FADP,
- Komisi Informasi Perlindungan Data Federal Swiss adalah otoritas pengawas yang kompeten sesuai Klausul 13 dan Lampiran I.C dari EU SCC
- Hukum Swiss sebagai hukum yang mengatur dalam hal transfer secara eksklusif tunduk pada FADP dan
- Syarat "status anggota" dalam Klausul 18 dari EU SCC harus diperluas untuk menyertakan Swiss dengan tujuan memungkinkan subjek data Swiss untuk mengupayakan hak mereka di tempat tinggal tetap mereka.

(b) For the avoidance of doubt, none of the above is intended to decrease the level of data protection provided by the EU SCC in any way, but only to extend this level of protection to Swiss data subjects. If and to the extend this is not the case, the EU SCC shall prevail.

(b) Untuk menghindari keraguan, tidak satu pun klausul di atas yang dimaksudkan untuk mengurangi tingkat perlindungan data yang diberikan oleh EU SCC dengan cara apa pun, tetapi hanya untuk memperluas tingkat perlindungan ini ke subjek data Swiss. Jika dan sejauh hal tersebut tidak demikian,

6. Assistance and Records

6.1 Taking into account the nature of Processing, Supplier will assist Kyndryl by having appropriate technical and organizational measures to fulfill obligations associated with Data Subject requests and rights. Supplier will also assist Kyndryl in ensuring compliance with obligations relating to the security of Processing, the notification and communication of a Security Breach and the creation of data protection impact assessments, including prior consultation with the responsible regulator, if required, taking into account the information available to Supplier.

6.2 Supplier will maintain an up-to-date record of the name and contact details of each Subprocessor, including each Subprocessor's representative and data protection officer. Upon request, Supplier will provide this record to Kyndryl on a schedule that allows Kyndryl to timely respond to any demand from a Customer or other third-party.

EU SCC akan diutamakan.

6. Bantuan dan Catatan

6.1 Mempertimbangkan karakteristik Pemrosesan, Pemasok akan membantu Kyndryl dengan menjalankan tindakan teknis dan organisasi yang sesuai untuk memenuhi kewajiban yang berkaitan dengan permintaan dan hak Subjek Data. Pemasok juga akan membantu Kyndryl dalam memastikan kepatuhan terhadap kewajiban yang berkaitan dengan keamanan Pemrosesan, pemberitahuan dan komunikasi Pelanggaran Keamanan dan pembuatan penilaian dampak perlindungan data, termasuk konsultasi sebelumnya dengan pembuat peraturan yang bertanggung jawab, apabila diperlukan, dengan mempertimbangkan informasi yang tersedia untuk Pemasok.

6.2 Pemasok akan mengelola catatan rincian nama dan kontak terbaru dari masing-masing Subprosesor, termasuk masing-masing perwakilan dan pejabat perlindungan data Subprosesor. Berdasarkan permintaan, Pemasok akan memberikan catatan ini kepada Kyndryl pada jadwal yang mengizinkan Kyndryl untuk menanggapi secara tepat waktu setiap permintaan dari Pelanggan atau pihak ketiga lainnya.

Article IV, Technical and Organizational Measures, Code Security

This Article applies if Supplier has access to Kyndryl Source Code. Supplier will comply with the requirements of this Article and by doing so protect Kyndryl Source Code against loss, destruction, alteration, accidental or unauthorized disclosure, accidental or unauthorized access, and unlawful forms of Handling. The requirements of this Article extend to all IT applications, platforms, and infrastructure that Supplier operates or manages in providing Deliverables and Services and in Handling Kyndryl Technology, including all development, testing, hosting, support, operations, and data center environments.

1. Security Requirements

As used below,

Prohibited Country means any country: (a) that the US Government has designated as a foreign adversary under the May 15, 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain, (b) listed in accordance with Section 1654 of the U.S. National Defense Authorization Act of 2019, or (c) identified as a "Prohibited Country" in the Transaction Document.

1.1 Supplier will not distribute or place any Kyndryl Source Code in escrow for the benefit of any third party.

1.2 Supplier will not permit any Kyndryl Source Code to reside on servers located in a Prohibited Country. Supplier will not permit anyone, including its Personnel, located in a Prohibited Country or visiting a Prohibited Country (for the extent of any such visit), for any reason whatsoever, to access or use any Kyndryl Source Code, regardless of where that Kyndryl Source Code is located globally, and Supplier will not permit any development, testing, or other work to occur in a Prohibited Country that would require such access or use.

Pasal IV, Tindakan Teknis dan Organisasi, Keamanan Kode

Pasal ini berlaku jika Pemasok memiliki akses ke Kode Sumber Kyndryl. Pemasok akan mematuhi persyaratan Pasal ini dan sekaligus melindungi Kode Sumber Kyndryl terhadap kerugian, kerusakan, perubahan, pengungkapan secara tidak sengaja atau tidak sah, akses secara tidak sengaja atau tidak sah, dan bentuk Penanganan yang melanggar hukum. Persyaratan Pasal ini menjangkau semua aplikasi, platform, dan infrastruktur TI yang dioperasikan atau dikelola oleh Pemasok dalam memberikan Materi yang Disampaikan dan Layanan, dan dalam Penanganan Teknologi Kyndryl, termasuk semua pengembangan, pengujian, hosting, dukungan, operasi, dan lingkungan pusat data.

1. Persyaratan Keamanan

Sebagaimana yang digunakan di bawah ini,

Negara yang Dilarang berarti setiap negara: (a) yang ditetapkan oleh Pemerintah AS sebagai musuh asing berdasarkan Perintah Eksekutif Mengenai Pengamanan Teknologi Informasi dan Komunikasi dan Rantai Pasokan Layanan (Executive Order on Securing the Information and Communications Technology and Services Supply Chain) tertanggal 15 Mei 2019 , (b) yang terdaftar sesuai dengan Bagian 1654 Undang-Undang Otorisasi Pertahanan A.S. (U.S. National Defense Authorization Act) 2019, atau (c) diidentifikasi sebagai "Negara yang Dilarang" dalam Dokumen Transaksi.

1.1 Pemasok tidak akan mendistribusikan atau menempatkan setiap Kode Sumber Kyndryl dalam penangguhan untuk kepentingan pihak ketiga mana pun.

1.2 Pemasok tidak akan mengizinkan setiap Kode Sumber Kyndryl untuk ditempatkan di server yang berlokasi di Negara yang Dilarang. Pemasok tidak akan mengizinkan siapa pun, termasuk Personelnya, yang berlokasi di Negara yang Dilarang atau mengunjungi Negara yang Dilarang (sejauh untuk kunjungan semacam itu), untuk alasan apa pun, mengakses atau menggunakan setiap Kode Sumber Kyndryl, terlepas dari lokasi Kode Sumber Kyndryl secara global, dan Pemasok tidak akan mengizinkan setiap pengembangan, pengujian, atau pekerjaan lain dilakukan di Negara yang Dilarang yang mungkin memerlukan akses atau penggunaan tersebut.

1.3 Supplier will not place or distribute Kyndryl Source Code in any jurisdiction where law or interpretation of law requires disclosure of Source Code to any third party. If there is a change of law or interpretation of law in a jurisdiction where Kyndryl Source Code is located that may cause Supplier to be required to disclose such Source Code to a third party, Supplier will immediately destroy or immediately remove such Kyndryl Source Code from such jurisdiction, and will not place any additional Kyndryl Source Code in such jurisdiction if such law or interpretation of law remains operative.

1.4 Supplier will not, directly or indirectly, take any action, including entering into any agreement, that would cause Supplier, Kyndryl or any third-party to incur a disclosure obligation under Sections 1654 or 1655 of the U.S. National Defense Authorization Act of 2019. For clarity, except as may be expressly permitted in the Transaction Document or associated base agreement between the parties, Supplier is not permitted to disclose Kyndryl Source Code to any third-party, under any circumstance, without Kyndryl's prior written consent.

1.5 If Kyndryl notifies Supplier, or a third party notifies either party that: (a) Supplier has allowed Kyndryl Source Code to be brought into a Prohibited Country or any jurisdiction subject to Section 1.3 above, (b) Supplier has otherwise released, accessed, or used Kyndryl Source Code in a manner not permitted by the Transaction Document or associated base or other agreement between the parties or (c) Supplier has violated Section 1.4 above, then without limiting Kyndryl's rights to address such non-compliance at law or in equity or under the Transaction Document or associated base or other agreement between the parties: (i) if such notification is to Supplier, then Supplier will promptly share the notification with Kyndryl; and (ii) Supplier, at Kyndryl's reasonable direction, will investigate and remediate the matter on the schedule that Kyndryl reasonably determines (after consultation with Supplier).

1.3 Pemasok tidak akan menempatkan atau mendistribusikan Kode Sumber Kyndryl di setiap yurisdiksi di mana hukum atau interpretasi hukum memerlukan pengungkapan Kode Sumber kepada pihak ketiga mana pun. Jika terdapat perubahan hukum atau interpretasi hukum dalam yurisdiksi di mana Kode Sumber Kyndryl berlokasi yang dapat menyebabkan Pemasok diwajibkan mengungkap Kode Sumber tersebut kepada pihak ketiga, Pemasok akan segera memusnahkan atau segera menghapus Kode Sumber Kyndryl tersebut dari yurisdiksi tersebut, dan tidak akan menempatkan setiap Kode Sumber Kyndryl tambahan di yurisdiksi tersebut jika hukum atau interpretasi hukum yang demikian masih berlaku.

1.4 Pemasok tidak akan, secara langsung atau tidak langsung, mengambil tindakan apa pun, termasuk menandatangani perjanjian apa pun, yang dapat menyebabkan Pemasok, Kyndryl, atau pihak ketiga mana pun terkena kewajiban pengungkapan berdasarkan Bagian 1654 atau 1655 Undang-Undang Otorisasi Pertahanan Nasional A.S. (U.S. National Defense Authorization Act) tahun 2019. Untuk kejelasan, kecuali sebagaimana yang dapat diizinkan secara tegas dalam Dokumen Transaksi atau perjanjian dasar terkait antara para pihak, Pemasok tidak diizinkan untuk mengungkap Kode Sumber Kyndryl kepada pihak ketiga mana pun, dalam situasi apa pun, tanpa persetujuan tertulis sebelumnya dari Kyndryl.

1.5 Jika Kyndryl memberi tahu Pemasok, atau pihak ketiga memberi tahu salah satu pihak bahwa: (a) Pemasok telah mengizinkan Kode Sumber Kyndryl untuk dibawa ke Negara yang Dilarang atau yurisdiksi mana pun dengan tunduk pada Bagian 1.3 di atas, (b) Pemasok telah merilis, mengakses, atau menggunakan Kode Sumber Kyndryl dengan cara yang tidak diizinkan dalam Dokumen Transaksi atau perjanjian dasar atau perjanjian terkait lainnya di antara para pihak atau (c) Pemasok telah melanggar Bagian 1.4 di atas, kemudian tanpa membatasi hak Kyndryl untuk menangani ketidakpatuhan tersebut menurut aturan hukum atau asas keadilan atau berdasarkan Dokumen Transaksi atau perjanjian dasar atau perjanjian lain yang terkait di antara para pihak: (i) jika pemberitahuan tersebut ditujukan kepada Pemasok, kemudian Pemasok akan segera membagikan pemberitahuan tersebut dengan Kyndryl; dan (ii) Pemasok, atas arahan Kyndryl yang wajar, akan menginvestigasi dan meremediasi permasalahan pada jadwal yang ditentukan oleh Kyndryl secara wajar (setelah konsultasi dengan

1.6 If Kyndryl reasonably believes that changes in Supplier's policies, procedures, controls, or practices with respect to Source Code access may be necessary to address cyber security, intellectual property theft or similar or related risks (including the risk that without such changes Kyndryl might be restricted from selling to certain Customers or into certain markets or otherwise be unable to satisfy Customer security or supply chain requirements), then Kyndryl may contact Supplier to discuss the actions necessary to address such risks, including changes to such policies, procedures, controls or practices. Upon Kyndryl's request, Supplier will cooperate with Kyndryl in evaluating whether such changes are necessary and in implementing appropriate, mutually agreed changes.

Pemasok).

1.6 Jika Kyndryl meyakini secara wajar bahwa perubahan dalam kebijakan, prosedur, kontrol, atau praktik Pemasok berkaitan dengan akses Kode Sumber mungkin diperlukan untuk menangani keamanan siber, pencurian kekayaan intelektual atau serupa itu atau risiko terkait (termasuk risiko bahwa tanpa perubahan tersebut Kyndryl mungkin dibatasi untuk menjual ke Pelanggan tertentu atau ke pasar tertentu atau sebaliknya tidak dapat memenuhi persyaratan keamanan atau rantai pasokan Pelanggan), maka Kyndryl dapat menghubungi Pemasok untuk membahas tindakan yang diperlukan untuk menangani risiko tersebut, termasuk perubahan pada kebijakan, prosedur, kontrol, atau praktik tersebut. Atas permintaan Kyndryl, Pemasok akan bekerja sama dengan Kyndryl dalam mengevaluasi apakah perubahan tersebut diperlukan dan dalam mengimplementasikan perubahan yang sesuai dan disetujui bersama.

Article V, Secure Development

This Article applies if Supplier will provide its or third-party Source Code or On-Premise Software to Kyndryl, or if any of Supplier's Deliverables or Services will be provided to an Kyndryl Customer as part of an Kyndryl product or service.

1. Security Readiness

1.1 Supplier will cooperate with Kyndryl's internal processes that assess the security readiness of Kyndryl products and services that are dependent upon any of Supplier's Deliverables, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Supplier Personnel, or the like.

2. Secure Development

2.1 This Section 2 only applies where Supplier is providing On-Premise Software to Kyndryl.

2.2 Supplier has implemented and will maintain throughout the term of the Transaction Document, in accordance with Industry Best Practices, the network, platform, system, application, device, physical infrastructure, incident response, and Personnel focused security policies, procedures, and controls that are necessary to protect: (a) the development, build, test and operations systems and environments that Supplier or any third-party engaged by Supplier operates, manages, uses or otherwise relies upon for or with respect to the Deliverables and (b) all Deliverable source code against loss, unlawful forms of handling, and unauthorized access, disclosure, or alteration.

3. ISO 20243 Certification

3.1 This Section 3 only applies if any of Supplier's Deliverables or Services will be provided to an Kyndryl Customer as part of an Kyndryl product or service.

3.2 Supplier will obtain a certification of compliance with ISO 20243, Information technology,

Pasal V, Pengembangan Aman

Pasal ini berlaku jika Pemasok akan memberikan Kode Sumbernya atau Kode Sumber pihak ketiga atau Perangkat Lunak di Lokasi kepada Kyndryl, atau jika ada Materi yang Disampaikan atau Layanan Pemasok yang akan diberikan kepada Pelanggan Kyndryl sebagai bagian dari produk atau layanan Kyndryl.

1. Kesiapan Keamanan

1.1 Pemasok akan bekerja sama dengan proses internal Kyndryl yang menilai kesiapan keamanan produk dan layanan Kyndryl yang bergantung pada setiap Materi yang Disampaikan Pemasok, termasuk menanggapi sepenuhnya dan tepat waktu atas permintaan informasi, baik melalui dokumen, catatan lain, wawancara Personel Pemasok terkait, atau semacamnya.

2. Pengembangan Aman

2.1 Bagian 2 ini hanya berlaku jika Pemasok memberikan Perangkat Lunak di Lokasi kepada Kyndryl.

2.2 Pemasok telah mengimplementasikan dan akan memelihara selama jangka waktu Dokumen Transaksi, sesuai dengan Praktik Terbaik Industri, jaringan, platform, sistem, aplikasi, perangkat, infrastruktur fisik, tanggapan insiden, dan kebijakan, prosedur, dan kontrol keamanan yang berfokus pada Personel yang diperlukan untuk melindungi: (a) sistem dan lingkungan pengembangan, pembuatan, pengujian, dan operasi di mana Pemasok atau pihak ketiga mana pun yang dilibatkan oleh Pemasok mengoperasikan, mengelola, menggunakan, atau mengandalkan pada atau sehubungan dengan Materi yang Disampaikan dan (b) semua kode sumber Materi yang Disampaikan terhadap kerugian, bentuk penanganan yang melanggar hukum, serta akses, pengungkapan, atau perubahan yang tidak sah.

3. Sertifikasi ISO 20243

3.1 Bagian 3 ini hanya berlaku jika ada Materi yang Disampaikan atau Layanan Pemasok yang akan diberikan kepada Pelanggan Kyndryl sebagai bagian dari produk atau layanan Kyndryl.

3.2 Pemasok akan mendapatkan sertifikasi kepatuhan dengan ISO 20243, Teknologi informasi,

Open Trusted Technology Provider, TM Standard (O-TTPS), Mitigating maliciously tainted and counterfeit products (either a self-assessed certification or one based on the assessment of a reputable independent auditor). In the alternative, if Supplier requests in writing and Kyndryl approves in writing, Supplier will obtain a certification of compliance with a substantially equivalent industry standard addressing secure development and supply chain practices (either a self-assessed certification or one based on the assessment of a reputable independent auditor, if and as Kyndryl approves).

Open Trusted Technology Provider, TM Standard (O-TTPS), Mitigasi produk yang tercemar dan palsu (sertifikasi yang dinilai secara mandiri atau yang didasarkan pada penilaian auditor independen yang bereputasi). Sebagai alternatif, jika Pemasok meminta secara tertulis dan Kyndryl menyetujui secara tertulis, Pemasok akan memperoleh sertifikasi kepatuhan dengan standar industri yang setara secara substansial yang menangani pengembangan aman dan praktik rantai pasokan (sertifikasi yang dinilai secara mandiri atau yang didasarkan pada penilaian auditor independen bereputasi, jika dan selama Kyndryl menyetujui).

3.3 Supplier will obtain the certification of compliance with ISO 20243 or a substantially equivalent industry standard (if Kyndryl approves in writing) by 180 Days after the effective date of the Transaction Document
and then renew the certification every 12 months thereafter (with each renewal against the then most current version of the applicable standard, i.e., ISO 20243 or, where Kyndryl has approved in writing, a substantially equivalent industry standard addressing secure development and supply chain practices).

3.3 Pemasok akan memperoleh sertifikasi kepatuhan dengan ISO 20243 atau standar industri yang setara secara substansial (jika Kyndryl menyetujui secara tertulis) paling lambat 180 Hari setelah tanggal mulai berlaku Dokumen Transaksi
dan kemudian memperbarui sertifikasi setiap 12 bulan setelahnya (dengan masing-masing pembaruan pada versi terbaru saat itu dari standar yang berlaku, yaitu ISO 20243 atau, jika Kyndryl telah menyetujui secara tertulis, standar industri yang setara secara substansial yang menangani pengembangan aman dan praktik rantai pasokan).

3.4 Supplier will, upon request, promptly provide to Kyndryl a copy of the certifications Supplier is obligated to obtain, per Sections 2.1 and 2.2 above.

3.4 Pemasok akan, berdasarkan permintaan, segera memberikan salinan sertifikasi yang wajib diperoleh oleh Pemasok kepada Kyndryl, sesuai Bagian 2.1 dan 2.2 di atas.

4. Security Vulnerabilities

As used below,

Error Correction means bug fixes and revisions that correct errors or deficiencies, including Security Vulnerabilities, in Deliverables.

Mitigation means any known means of lessening or avoiding the risks of a Security Vulnerability.

Security Vulnerability means a state in the design, coding, development, implementation, testing, operation, support, maintenance, or management of a Deliverable that allows an attack by anyone that could result in unauthorized access or exploitation, including: (a) access to, controlling or disrupting operation of a system, (b) access to, deleting, altering

4. Kerentanan Keamanan

Sebagaimana yang digunakan di bawah ini,

Koreksi Kesalahan berarti perbaikan bug dan revisi yang mengoreksi kesalahan atau defisiensi, termasuk Kerentanan Keamanan, dalam Materi yang Disampaikan.

Mitigasi berarti setiap cara yang diketahui untuk mengurangi atau menghindari risiko Kerentanan Keamanan.

Kerentanan Keamanan berarti kondisi dalam desain, pengodean, pengembangan, implementasi, pengujian, pengoperasian, dukungan, pemeliharaan, atau manajemen Materi yang Disampaikan yang mengizinkan serangan oleh siapa pun yang dapat berakibat pada akses atau eksploitasi yang tidak sah, termasuk: (a) akses ke, kontrol atau gangguan operasi sistem , (b) akses ke, penghapusan, pengubahan atau

or extracting data or (c) changes of identity, authorizations or permissions of users or administrators. A Security Vulnerability may exist regardless of whether a Common Vulnerabilities and Exposures (CVE) ID or any scoring or official classification is assigned to it.

ekstraksi data atau (c) perubahan identitas, otorisasi atau izin pengguna atau administrator. Kerentanan Keamanan mungkin ada terlepas dari apakah ID Kerentanan dan Eksposur Umum (Common Vulnerabilities and Exposures - CVE) atau setiap pemberian skor atau klasifikasi resmi ditetapkan untuknya.

4.1 Supplier represents and warrants that it will: (a) use Industry Best Practices to identify Security Vulnerabilities, including through continuous static and dynamic source code application security scanning, open source security scanning and system vulnerability scanning, and (b) comply with the requirements of these Terms to help prevent, detect and correct Security Vulnerabilities in Deliverables and in all IT applications, platforms, and infrastructure in and through which Supplier creates and provides Services and Deliverables.

4.1 Pemasok menyatakan dan menjamin bahwa pihaknya akan: (a) menggunakan Praktik Terbaik Industri untuk mengidentifikasi Kerentanan Keamanan, termasuk melalui pemindaian keamanan aplikasi kode sumber statis dan dinamis berkelanjutan, pemindaian keamanan sumber terbuka dan pemindaian kerentanan sistem, dan (b) mematuhi persyaratan dari Syarat-Syarat ini untuk membantu mencegah, mendeteksi, dan melakukan koreksi Kerentanan Keamanan pada Materi yang Disampaikan dan di semua aplikasi, platform, dan infrastruktur TI di mana dan selama Pemasok membuat dan memberikan Layanan dan Materi yang Disampaikan.

4.2 If Supplier becomes aware of a Security Vulnerability in a Deliverable or any such IT application, platform, or infrastructure, Supplier will provide Kyndryl with an Error Correction and Mitigations for all versions and releases of the Deliverables in accordance with the Severity Levels and time frames defined in the tables below:

4.2 Apabila Pemasok menyadari adanya Kerentanan Keamanan dalam Materi yang Disampaikan atau setiap aplikasi, platform, atau infrastruktur TI tersebut, Pemasok akan memberikan Koreksi Kesalahan dan Mitigasi kepada Kyndryl untuk semua versi dan rilis Materi yang Disampaikan sesuai dengan Tingkat Keamanan dan kerangka waktu yang ditentukan dalam tabel di bawah ini:

Severity Level*/ ***Tingkat Keamanan****
Emergency Security Vulnerability – is a Security Vulnerability that constitutes a severe and potentially global threat. Kyndryl designates Emergency Security Vulnerabilities in its sole discretion, regardless of CVSS Base Score./ ***Kerentanan Keamanan Darurat*** *– adalah Kerentanan Keamanan yang merupakan ancaman berat dan berpotensi secara global. Kyndryl menetapkan Kerentanan Keamanan Darurat dalam kebijakan tunggalnya, terlepas dari Skor Dasar CVSS.*
Critical – is a Security Vulnerability that has a CVSS Base Score from 9 to 10.0/ ***Kritis*** *– yaitu Kerentanan Keamanan yang memiliki Skor Dasar CVSS dari 9 hingga 10,0*
High – is a Security Vulnerability that has a CVSS Base Score from 7.0 to 8.9/ ***Tinggi*** *– yaitu Kerentanan Keamanan yang memiliki Skor Dasar CVSS dari 7,0 hingga 8,9*
Medium – is a Security Vulnerability that has a CVSS Base Score from 4.0 to 6.9/ ***Sedang*** *– yaitu Kerentanan Keamanan yang memiliki Skor Dasar CVSS dari 4,0 hingga 6,9*
Low – is a Security Vulnerability that has a CVSS Base Score from 0.0 to 3.9/ ***Rendah*** *– yaitu Kerentanan Keamanan yang memiliki Skor Dasar CVSS dari 0,0 hingga 3,9*

Time Frames/ *Kerangka Waktu*				
Emergency/ Darurat	***Critical/ Kritis***	***High/ Tinggi***	***Medium/ Sedang***	***Low/ Rendah***
4 Days or less, as determined by Kyndryl's	30 Days/ *30 Hari*	30 Days/ *30 Hari*	90 Days/ *90 Hari*	Per Industry Best Practices/

Chief Information Security Office/ 4 Hari atau kurang, sebagaimana yang ditentukan oleh Kantor Kepala Keamanan Informasi (Chief Information Security Office) Kyndryl				*Sesuai Praktik Terbaik Industri*

* In any case where a Security Vulnerability does not have a readily assigned CVSS Base Score, Supplier will apply a Severity Level that is appropriate for the nature and circumstances of such vulnerability.

4.3 For a Security Vulnerability that has been publicly disclosed and for which Supplier has not yet provided any Error Correction or Mitigation to Kyndryl, Supplier will implement any technically feasible additional security controls that may mitigate the risks of the vulnerability.

4.4 If Kyndryl is dissatisfied with Supplier's response to any Security Vulnerability in a Deliverable or any application, platform, or infrastructure referenced above, then without prejudice to any other rights of Kyndryl, Supplier will promptly arrange for Kyndryl to discuss its concerns directly with a Supplier Vice President or equivalent executive that is responsible for delivery of the Error Correction.

4.5 Examples of Security Vulnerabilities include third-party code or end-of-service (EOS) open source code, where these types of code no longer receive security fixes.

* Apabila Kerentanan Keamanan tidak memiliki Skor Dasar CVSS yang siap ditetapkan, Pemasok akan mengajukan Tingkat Permasalahan yang sesuai untuk sifat dan keadaan kerentanan tersebut.

4.3 Untuk Kerentanan Keamanan yang telah diungkapkan kepada publik dan yang untuknya Pemasok belum memberikan Koreksi Kesalahan atau Mitigasi kepada Kyndryl, Pemasok akan mengimplementasikan setiap kontrol keamanan tambahan yang layak secara teknis yang dapat memitigasi risiko kerentanan.

4.4 Apabila Kyndryl tidak puas dengan tanggapan Pemasok atas setiap Kerentanan Keamanan dalam Materi yang Disampaikan atau setiap aplikasi, platform, atau infrastruktur yang direferensikan di atas, maka tanpa prasangka pada setiap hak Kyndryl lainnya, Pemasok akan segera mengatur Kyndryl untuk mendiskusikan persoalannya secara langsung dengan Wakil Direktur Pemasok atau eksekutif yang setara yang bertanggung jawab atas penyampaian Koreksi Kesalahan.

4.5 Contoh Kerentanan Keamanan termasuk kode pihak ketiga atau kode sumber terbuka end-of-service ("EOS"), di mana tipe kode ini sudah tidak lagi menerima perbaikan keamanan.

Article VI, Corporate Systems' Access

This Article applies if Supplier employees will have access to any Corporate System.

1. General Terms

1.1 Kyndryl will determine whether to authorize Supplier employees to access Corporate Systems. If Kyndryl so authorizes, then Supplier will comply, and will cause its employees with such access to comply, with the requirements of this Article.

1.2 Kyndryl will identify the means by which Supplier employees may access Corporate Systems, including whether such employees will access Corporate Systems through Kyndryl or Supplier provided Devices.

1.3 Supplier employees may only access Corporate Systems, and may only use the Devices that Kyndryl authorizes for that access, to provide Services. Supplier employees may not use the Devices that Kyndryl so authorizes to provide services to any other person or entity, or to access any Supplier or third-party IT systems, networks, applications, websites, email tools, collaboration tools, or the like for or in connection with the Services.

1.4 For clarity, Supplier employees may not use the Devices that Kyndryl authorizes to access Corporate Systems for any personal reason (e.g., Supplier employees may not store personal files such as music, videos, pictures or other like items on such Devices and cannot use the Internet from such Devices for personal reasons).

1.5 Supplier employees will not copy Kyndryl Materials that are accessible through a Corporate System without Kyndryl's prior written approval (and will never copy any Kyndryl Materials to a portable storage device, such as a USB, an external hard drive, or other like items).

1.6 Upon request, Supplier will confirm, by employee name, the specific Corporate Systems which its employees are authorized to access, and have accessed, over any time period that Kyndryl identifies.

Pasal VI, Akses Sistem Korporasi

Pasal ini berlaku jika karyawan Pemasok akan memiliki akses ke setiap Sistem Korporasi.

1. Syarat-Syarat Umum

1.1 Kyndryl akan menentukan apakah akan mengotorisasi karyawan Pemasok untuk mengakses Sistem Korporasi. Jika Kyndryl memberi wewenang, maka Pemasok akan mematuhi, dan akan menjadikan karyawannya yang memiliki akses untuk patuh dengan persyaratan Pasal ini.

1.2 Kyndryl akan mengidentifikasi cara yang digunakan karyawan Pemasok untuk dapat mengakses Sistem Korporasi, termasuk apakah karyawan tersebut akan mengakses Sistem Korporasi melalui Perangkat yang disediakan Kyndryl atau Pemasok.

1.3 Karyawan pemasok hanya dapat mengakses Sistem Korporasi, dan hanya dapat menggunakan Perangkat yang disahkan oleh Kyndryl untuk akses tersebut, untuk memberikan Layanan. Karyawan pemasok tidak dapat menggunakan Perangkat yang disahkan Kyndryl untuk memberikan layanan kepada setiap orang atau entitas lain, atau untuk, mengakses setiap sistem, jaringan, aplikasi, situs web, alat email, alat kolaborasi TI atau semacamnya milik Pemasok atau pihak ketiga untuk atau berkaitan dengan Layanan.

1.4 Untuk kejelasan, karyawan Pemasok tidak dapat menggunakan Perangkat yang disahkan Kyndryl untuk mengakses Sistem Korporasi untuk alasan pribadi apa pun (misalnya, karyawan Pemasok tidak dapat menyimpan file pribadi seperti musik, video, gambar atau item serupa lainnya pada Perangkat tersebut dan tidak dapat menggunakan Internet dari Perangkat tersebut).

1.5 Karyawan Pemasok tidak akan menyalin Materi Kyndryl yang dapat diakses melalui Sistem Korporasi tanpa persetujuan tertulis sebelumnya dari Kyndryl (dan tidak akan pernah menyalin setiap Materi Kyndryl ke perangkat penyimpanan portabel, seperti USB, hard drive eksternal, atau item serupa lainnya).

1.6 Berdasarkan permintaan, Pemasok akan mengonfirmasi, berdasarkan nama karyawan, Sistem Korporasi spesifik di mana karyawannya diberi wewenang untuk mengakses, dan telah mengakses, selama periode waktu kapan pun yang diidentifikasi Kyndryl.

1.7 Supplier will notify Kyndryl within twenty-four (24) hours after any Supplier employee with access to any Corporate System is no longer: (a) employed by Supplier or (b) working on activities that require such access. Supplier will work with Kyndryl to ensure that access for such former or current employees is immediately revoked.

1.8 Supplier will immediately report any actual or suspected security incidents (such as loss of an Kyndryl or Supplier Device or unauthorized access to a Device or data, materials or other information of any kind) to Kyndryl and cooperate with Kyndryl in the investigation of such incidents.

1.9 Supplier may not permit any agent, independent contractor or subcontractor employee to access any Corporate System, without Kyndryl's prior written consent; if Kyndryl provides that consent, then Supplier will contractually commit those persons and their employers to comply with the requirements of this Article as if those persons were Supplier employees, and will be responsible to Kyndryl for all actions and omissions to act by any such person or employer with respect to such Corporate System access.

2. Device Software

2.1 Supplier will direct its employees to timely install all Device software that Kyndryl requires to facilitate access to Corporate Systems in a secure manner. Neither Supplier nor its employees will interfere with the operations of that software or the security features that the software enables.

2.2 Supplier and its employees will adhere to the Device configuration rules that Kyndryl sets and otherwise work with Kyndryl to help ensure that the software functions as Kyndryl intends. For example, Supplier will not override software website blocking or automated patching features.

2.3 Supplier employees may not share the Devices they use to access Corporate Systems, or their Device user-names, passwords, or the like, with any other person.

1.7 Pemasok akan memberi tahu Kyndryl dalam dua puluh empat (24) jam setelah setiap karyawan Pemasok dengan akses ke setiap Sistem Korporasi tidak lagi: (a) dipekerjakan oleh Pemasok atau (b) bekerja pada aktivitas yang memerlukan akses tersebut. Pemasok akan bekerja dengan Kyndryl untuk memastikan bahwa akses untuk mantan karyawan atau karyawan saat ini segera dicabut.

1.8 Pemasok akan segera melaporkan setiap insiden keamanan aktual atau dugaan (seperti kehilangan Perangkat Kyndryl atau Pemasok atau akses yang tidak sah ke Perangkat atau data, materi atau informasi lain dalam bentuk apa pun) kepada Kyndryl dan bekerja sama dengan Kyndryl dalam investigasi insiden tersebut.

1.9 Pemasok tidak dapat mengizinkan setiap agen, kontraktor independen atau karyawan subkontraktor untuk mengakses setiap Sistem Korporasi tanpa izin tertulis dari Kyndryl sebelumnya; jika Kyndryl memberikan persetujuan tersebut, Pemasok akan menjamin orang tersebut dan karyawan mereka secara kontraktual untuk mematuhi persyaratan Pasal ini sebagaimana orang tersebut merupakan karyawan Pemasok, dan akan bertanggung jawab kepada Kyndryl untuk semua tindakan dan kelalaian dalam bertindak oleh orang atau karyawan mana pun tersebut sehubungan dengan akses Sistem Korporasi tersebut.

2. Perangkat Lunak Perangkat

2.1 Pemasok akan mengarahkan karyawannya untuk memasang semua perangkat lunak Perangkat yang disyaratkan oleh Kyndryl untuk memfasilitasi akses ke Sistem Korporasi dengan cara yang aman secara tepat waktu. Baik Pemasok maupun karyawannya tidak akan mengganggu operasi perangkat lunak atau fitur keamanan yang diaktifkan perangkat lunak.

2.2 Pemasok dan karyawannya akan mengikuti aturan konfigurasi Perangkat yang ditetapkan Kyndryl dan sebaliknya bekerja dengan Kyndryl untuk membantu memastikan bahwa perangkat lunak berfungsi sebagaimana yang dikehendaki oleh Kyndryl. Misalnya, Pemasok tidak akan menimpa pemblokiran situs web perangkat lunak atau fitur patching otomatis.

2.3 Karyawan pemasok tidak dapat membagikan Perangkat yang mereka gunakan untuk mengakses Sistem Korporasi, atau nama-pengguna, kata sandi, atau sejenisnya dari Perangkat mereka, dengan siapa pun.

2.4 If Kyndryl authorizes Supplier employees to access Corporate Systems using Supplier Devices, then Supplier will install and run an operating system on those Devices that Kyndryl approves and will upgrade to a new version of that operating system or a new operating system within a reasonable time after Kyndryl so instructs.

2.4 Jika Kyndryl memberi wewenang kepada karyawan Pemasok untuk mengakses Sistem Korporasi menggunakan Perangkat Pemasok, Pemasok akan memasang dan menjalankan sistem operasi pada Perangkat tersebut yang disetujui oleh Kyndryl dan akan memutakhirkan ke versi terbaru dari sistem operasi tersebut atau sistem operasi baru dalam waktu yang wajar setelah Kyndryl memberikan instruksi.

3. Oversight and Cooperation

3.1 Kyndryl has the unqualified rights to monitor and remediate potential intrusion and other cyber security threats in whatever ways, from whatever locations, and using whatever means Kyndryl believes is necessary or appropriate, without prior notice to Supplier or any Supplier employee or others. As examples of such rights, Kyndryl may, at any time, (a) perform a security test on any Device, (b) monitor, recover through technical or other means and review communications (including emails from any email accounts), records, files, and other items stored in any Device or transmitted through any Corporate System, and (c) acquire a full forensic image of any Device. If Kyndryl needs Supplier's cooperation to exercise its rights, Supplier will fully and timely satisfy Kyndryl's requests for such cooperation (including, for example, requests to securely configure any Device, install monitoring or other software on any Device, share system level connection details, engage in incident response measures on any Device, and provide physical access to any Device for Kyndryl to obtain a full forensic image or otherwise, and similar and related requests).

3. Kesalahan dan Kerja Sama

3.1 Kyndryl memiliki hak yang tidak memenuhi syarat untuk memantau dan memperbaiki potensi intrusi dan ancaman keamanan siber lainnya dalam cara apa pun, dari lokasi mana pun, dan menggunakan sarana apa pun yang diyakini Kyndryl perlu atau sesuai, tanpa pemberitahuan sebelumnya kepada Pemasok atau setiap karyawan Pemasok atau pihak lainnya. Sebagai contoh dari hak tersebut, Kyndryl dapat, kapan pun, (a) menjalankan uji keamanan pada Perangkat apa pun, (b) memantau, memulihkan melalui sarana teknis atau lainnya dan meninjau komunikasi (termasuk email dari setiap akun email), catatan, file, dan item lain yang disimpan di Perangkat apa pun atau ditransmisikan melalui setiap Sistem Korporasi, dan (c) memperoleh gambar forensik penuh dari setiap Perangkat. Jika Kyndryl memerlukan kerja sama Pemasok untuk melaksanakan haknya, Pemasok akan memenuhi permintaan Kyndryl sepenuhnya dan tepat waktu untuk kerja sama tersebut (termasuk, misalnya, permintaan untuk mengonfigurasi Perangkat apa pun dengan aman, memasang perangkat lunak pemantauan atau lainnya pada Perangkat apa pun, membagikan rincian koneksi tingkat sistem, terikat dalam tindakan tanggapan insiden pada Perangkat apa pun, dan memberikan akses fisik ke Perangkat apa pun untuk Kyndryl guna memperoleh gambar forensik penuh atau sebaliknya, dan permintaan terkait dan serupa).

3.2 Kyndryl may revoke access to Corporate Systems at any time, for any Supplier employee or all Supplier employees, without prior notice to Supplier or any Supplier employee or others, if Kyndryl believes that doing so is necessary to protect Kyndryl.

3.2 Kyndryl dapat mencabut akses ke Sistem Korporasi kapan pun, untuk setiap karyawan Pemasok atau semua karyawan Pemasok, tanpa pemberitahuan sebelumnya kepada Pemasok atau setiap karyawan Pemasok atau pihak lainnya, jika Kyndryl meyakini bahwa tindakan tersebut diperlukan untuk melindungi Kyndryl.

3.3 Kyndryl's rights are not blocked, lessened, or restricted in any way by any provision of the Transaction Document, the associated base agreement between the parties, or any other agreement between the parties, including any provision that may require data, materials or other information of any kind to reside only in a select location or locations or that may require that only persons from a select location or

3.3 Hak Kyndryl tidak diblokir, dikurangi, atau dibatasi dengan cara apa pun dengan setiap ketentuan dari Dokumen Transaksi, perjanjian dasar terkait di antara para pihak, atau perjanjian apa pun lainnya di antara para pihak, termasuk setiap ketentuan yang dapat memerlukan data, materi atau informasi lainnya dalam bentuk apa pun untuk ditempatkan hanya di lokasi terpilih atau yang mungkin mensyaratkan bahwa

locations access such data, materials or other information.

hanya orang-orang dari lokasi terpilih yang dapat mengakses data, materi atau informasi lainnya.

4. Kyndryl Devices

4. Perangkat Kyndryl

4.1 Kyndryl will retain title to all Kyndryl Devices, with Supplier bearing the risk of loss of the Devices, including due to theft, vandalism, or negligence. Supplier will not make or permit any alterations to Kyndryl Devices without Kyndryl's prior written consent, with an alteration being any change to a Device, including any change to Device software, applications, security design, security configuration, or physical, mechanical, or electrical design.

4.1 Kyndryl akan memegang hak milik atas semua Perangkat Kyndryl, sementara Pemasok menanggung risiko kerugian Perangkat, termasuk karena pencurian, vandalisme, atau kelalaian. Pemasok tidak akan membuat atau mengizinkan perubahan apa pun terhadap Perangkat Kyndryl tanpa persetujuan tertulis sebelumnya dari Kyndryl, dengan perubahan tersebut adalah perubahan apa pun pada Perangkat, termasuk setiap perubahan pada perangkat lunak, aplikasi, desain keamanan, konfigurasi keamanan, atau desain fisik, mekanis, atau elektrik dari Perangkat.

4.2 Supplier will return all Kyndryl Devices within 5 business days after the need for those Devices to provide Services ends, and if Kyndryl requests, destroy all data, materials and other information of any kind on those Devices at the same time, without retaining any copy, by following Industry Best Practices to permanently erase all such data, materials and other information. Supplier will pack and return Kyndryl Devices in the same condition as delivered to Supplier, other than reasonable wear and tear, at its own expense to the location that Kyndryl identifies. Supplier's failure to comply with any obligation in this Section 4.2 constitutes a material breach of the Transaction Document and associated base agreement and any related agreement between the parties, with the understanding that an agreement is "related" if access to any Corporate System facilitates Supplier's tasks or other activities under that agreement.

4.2 Pemasok akan mengembalikan semua Perangkat Kyndryl dalam 5 hari kerja setelah kebutuhan untuk Perangkat tersebut guna memberikan Layanan berakhir, dan jika Kyndryl meminta, memusnahkan semua data, materi, dan informasi lainnya dalam bentuk apa pun pada Perangkat tersebut pada waktu yang sama, tanpa menyimpan salinan apa pun, dengan mengikuti Praktik Terbaik Industri untuk menghapus secara permanen semua data, materi, informasi lainnya tersebut. Pemasok akan mengemas dan mengembalikan Perangkat Kyndryl dalam kondisi yang sama sebagaimana ketika dikirimkan kepada Pemasok, selain keausan yang wajar, dengan biaya sendiri ke lokasi yang diidentifikasi Kyndryl. Kegagalan Pemasok untuk mematuhi setiap kewajiban dalam Bagian 4.2 ini merupakan pelanggaran material terhadap Dokumen Transaksi dan perjanjian dasar yang terkait dan setiap perjanjian terkait di antara para pihak, dengan pemahaman bahwa suatu perjanjian "terkait" jika akses ke setiap Sistem Korporasi memfasilitasi tugas Pemasok atau aktivitas lainnya berdasarkan perjanjian tersebut.

4.3 Kyndryl will provide support for Kyndryl Devices (including Device inspection and preventive and remedial maintenance). Supplier will promptly advise Kyndryl of the need for remedial service.

4.3 Kyndryl akan memberikan dukungan untuk Perangkat Kyndryl (termasuk pemeriksaan serta pemeliharaan preventif dan perbaikan Perangkat). Pemasok akan segera menyarankan Kyndryl mengenai keperluan untuk layanan perbaikan.

4.4. For software programs that Kyndryl owns or has the right to license, Kyndryl grants Supplier a temporary right to use, store, and make sufficient copies to support its authorized use of Kyndryl Devices. Supplier may not transfer programs to anyone, make copies of software license information, or disassemble, decompile, reverse engineer, or otherwise translate any program unless expressly permitted by applicable law without the possibility of contractual waiver.

4.4. Untuk program perangkat lunak yang dimiliki oleh Kyndryl atau memiliki hak untuk melisensikan, Kyndryl memberikan kepada Pemasok hak sementara untuk menggunakan, menyimpan, dan membuat salinan yang memadai untuk mendukung penggunaannya yang sah atas Perangkat Kyndryl. Pemasok tidak dapat mentransfer program kepada siapa pun, membuat salinan informasi lisensi perangkat lunak, atau membongkar, mendekompilasi, merekayasa balik, atau menerjemahkan setiap program kecuali apabila

5. Updates

5.1 Notwithstanding anything to the contrary in the Transaction Document or associated base agreement between the parties, upon written notice to Supplier and without the need for obtaining Supplier's consent, Kyndryl may update, supplement, or otherwise amend this Article to address any requirement under applicable law or Customer obligation, to reflect any development in security best practices, or otherwise as Kyndryl believes necessary to protect Corporate Systems or Kyndryl.

diizinkan secara tegas oleh hukum yang berlaku tanpa kemungkinan pengabaian kontraktual.

5. Pembaruan

5.1 Terlepas dari ketentuan apa pun yang bertentangan dalam Dokumen Transaksi atau perjanjian dasar terkait di antara para pihak, setelah pemberitahuan tertulis kepada Pemasok dan tanpa perlu memperoleh persetujuan Pemasok, Kyndryl dapat memperbarui, menambah, atau mengubah Pasal ini untuk mengurus setiap persyaratan berdasarkan hukum yang berlaku atau kewajiban Pelanggan, untuk merefleksikan setiap pengembangan dalam praktik terbaik keamanan, atau sebagaimana yang Kyndryl yakini perlu untuk melindungi Sistem Korporasi atau Kyndryl.

Article VII, Staff Augmentation

This Article applies where Supplier's employees will devote all of their working time to provide Services for Kyndryl, will perform all of those Services on Kyndryl premises, Customer premises or from their homes, and will only provide Services using Kyndryl Devices to access Corporate Systems.

1. Access to Corporate Systems; Kyndryl's Environments

1.1 Supplier may only perform Services by accessing Corporate Systems using Devices that Kyndryl provides.

1.2 Supplier will comply with the terms set forth in Article VI (Corporate Systems' Access), for all access to Corporate Systems.

1.3 Kyndryl provided Devices are the only Devices that Supplier and its employees may use to provide Services and may only be used by Supplier and its employees to provide Services. For clarity, in no event may Supplier or its employees use any other devices to provide Services or use Kyndryl Devices for any other Supplier customer or for any purpose other than providing Services to Kyndryl.

1.4 Supplier employees using Kyndryl Devices may share Kyndryl Materials with each other and store such materials on the Kyndryl Devices, but only to the limited extent that such sharing and storage is necessary to successfully perform Services.

1.5 Except with respect to such storage within the Kyndryl Devices, in no event may Supplier or its employees remove any Kyndryl Materials from the Kyndryl repositories, environments, tools or infrastructure where they are retained by Kyndryl.

1.6 For clarity, Supplier and its employees are not authorized to transfer any Kyndryl Materials to any Supplier repositories, environments, tools, or infrastructure, or any other Supplier systems,

Pasal VII, Penambahan Staf

Pasal ini berlaku jika karyawan Pemasok akan menyerahkan semua waktu kerja mereka untuk memberikan Layanan untuk Kyndryl, akan menjalankan semua Layanan tersebut di lokasi Kyndryl, lokasi Pelanggan atau dari rumah mereka, dan hanya akan memberikan Layanan menggunakan Perangkat Kyndryl untuk mengakses Sistem Korporasi.

1. Akses ke Sistem Korporasi; Lingkungan Kyndryl

1.1 Pemasok hanya dapat menjalankan Layanan dengan mengakses Sistem Korporasi menggunakan Perangkat yang diberikan Kyndryl.

1.2 Pemasok akan mematuhi syarat-syarat yang tercantum dalam Pasal VI (Akses Sistem Korporasi), untuk semua akses ke Sistem Korporasi.

1.3 Perangkat yang diberikan Kyndryl adalah satu-satunya Perangkat yang dapat digunakan oleh Pemasok dan karyawannya untuk menyediakan Layanan dan hanya dapat digunakan oleh Pemasok dan karyawannya untuk menyediakan Layanan. Untuk kejelasan, dalam hal apa pun Pemasok atau karyawannya tidak dapat menggunakan perangkat apa pun lainnya untuk menyediakan Layanan atau menggunakan Perangkat Kyndryl untuk setiap pelanggan Pemasok lainnya atau untuk setiap tujuan selain menyediakan Layanan kepada Kyndryl.

1.4 Karyawan pemasok yang menggunakan Perangkat Kyndryl dapat membagikan Materi Kyndryl satu sama lain dan menyimpan materi tersebut pada Perangkat Kyndryl, tetapi hanya sebatas aktivitas berbagi dan penyimpanan tersebut diperlukan untuk berhasil menjalankan Layanan.

1.5 Kecuali sehubungan dengan penyimpanan tersebut dalam Perangkat Kyndryl, dalam hal apa pun Pemasok atau karyawannya tidak dapat menghapus setiap Materi Kyndryl dari repositori, lingkungan, alat, atau infrastruktur Kyndryl di mana mereka disimpan oleh Kyndryl.

1.6 Untuk kejelasan, Pemasok dan karyawannya tidak diberi wewenang untuk mentransfer setiap Materi Kyndryl ke setiap repositori, lingkungan, alat, atau infrastruktur Pemasok atau setiap sistem, platform, jaringan, atau

platforms, networks or the like, without Kyndryl's prior written consent.

1.7 Article VIII (Technical and Organizational Measures, General Security) does not apply to Supplier's Services where Supplier's employees will devote all of their working time to provide Services for Kyndryl, will perform all of those Services on Kyndryl premises, Customer premises or from their homes, and will only provide Services using Kyndryl Devices to access Corporate Systems. Otherwise, Article VIII applies to Supplier's Services.

sejenisnya yang lain dari Pemasok, tanpa persetujuan tertulis sebelumnya dari Kyndryl.

1.7 Pasal VIII (Tindakan Teknis dan Organisasi, Keamanan Umum) tidak berlaku untuk Layanan Pemasok jika karyawan Pemasok akan menyerahkan semua waktu kerja mereka untuk memberikan Layanan untuk Kyndryl, akan menjalankan semua Layanan tersebut di lokasi Kyndryl, lokasi Pelanggan atau dari rumah mereka, dan hanya akan memberikan Layanan menggunakan Perangkat Kyndryl untuk mengakses Sistem Korporasi. Atau, Pasal VIII berlaku untuk Layanan Pemasok.

Article VIII, Technical and Organizational Measures, General Security

This Article applies if Supplier provides any Services or Deliverables to Kyndryl, unless Supplier will only have access to Kyndryl BCI in providing those Services and Deliverables (i.e., Supplier will not Process any other Kyndryl Data or have access to any other Kyndryl Materials or to any Corporate System), Supplier's only Services and Deliverables are to provide On-Premise Software to Kyndryl, or Supplier provides all of its Services and Deliverables in a staff augmentation model pursuant to Article VII, including Section 1.7 thereof.

Supplier will comply with the requirements of this Article and by doing so protect: (a) Kyndryl Materials against loss, destruction, alteration, accidental or unauthorized disclosure, and accidental or unauthorized access, (b) Kyndryl Data from unlawful forms of Processing and (c) Kyndryl Technology from unlawful forms of Handling. The requirements of this Article extend to all IT applications, platforms, and infrastructure that Supplier operates or manages in providing Deliverables and Services and in Handling Kyndryl Technology, including all development, testing, hosting, support, operations, and data center environments.

1. Security Policies

1.1 Supplier will maintain and follow IT security policies and practices that are integral to Supplier's business, mandatory for all Supplier Personnel, and consistent with Industry Best Practices.

1.2 Supplier will review its IT security policies and practices at least annually and amend them as Supplier deems necessary to protect the Kyndryl Materials.

1.3 Supplier will maintain and follow standard, mandatory employment verification requirements for all new employee hires, and extend such requirements to all Supplier Personnel and wholly-owned Supplier subsidiaries. Those requirements will include criminal background checks to the extent permitted by local laws, proof of identity validation, and additional checks that Supplier deems necessary. Supplier will periodically repeat and revalidate these requirements, as it deems necessary.

Pasal VIII, Tindakan Teknis dan Organisasi, Keamanan Umum

Pasal ini berlaku jika Pemasok memberikan setiap Layanan atau Materi yang Disampaikan kepada Kyndryl, kecuali jika Pemasok hanya akan memiliki akses ke BCI Kyndryl dalam memberikan Layanan dan Materi yang Disampaikan tersebut (yaitu, Pemasok tidak akan Memproses Data Kyndryl apa pun lainnya atau memiliki akses ke Materi Kyndryl apa pun lainnya atau ke Sistem Perusahaan mana pun), satu-satunya Layanan dan Materi yang Disampaikan Pemasok adalah untuk memberikan Perangkat Lunak di Lokasi kepada Kyndryl, atau Pemasok memberikan semua Layanan dan Materi yang Disampaikannya dalam model penambahan staf sesuai dengan Pasal VII, termasuk Bagian 1.7 tersebut.

Pemasok akan mematuhi persyaratan Pasal ini dan sekaligus melindungi: (a) Materi Kyndryl terhadap kehilangan, kerusakan, perubahan, pengungkapan secara tidak sengaja atau tidak sah, dan akses secara tidak sengaja atau tidak sah, (b) Data Kyndryl dari bentuk Pemrosesan yang melanggar hukum dan (c) Teknologi Kyndryl dari bentuk Penanganan yang melanggar hukum. Persyaratan Pasal ini menjangkau semua aplikasi, platform, dan infrastruktur TI yang dioperasikan atau dikelola oleh Pemasok dalam memberikan Materi yang Disampaikan dan Layanan, dan dalam Penanganan Teknologi Kyndryl, termasuk semua pengembangan, pengujian, hosting, dukungan, operasi, dan lingkungan pusat data.

1. Kebijakan Keamanan

1.1 Pemasok akan mempertahankan dan mengikuti praktik dan kebijakan keamanan TI yang melengkapi bisnis Pemasok, wajib untuk semua Personel Pemasok, dan sesuai dengan Praktik Terbaik Industri.

1.2 Pemasok akan meninjau kebijakan dan praktik keamanan TI-nya setidaknya setiap tahun dan mengubahnya jika dianggap perlu oleh Pemasok untuk melindungi Materi Kyndryl.

1.3 Pemasok akan mempertahankan dan mengikuti persyaratan verifikasi hubungan kerja standar dan wajib untuk semua perekrutan karyawan baru, dan memperluas persyaratan tersebut untuk semua Personel dan anak perusahaan Pemasok yang dimiliki seluruhnya. Persyaratan tersebut akan mencakup pemeriksaan latar belakang kriminal sejauh yang diizinkan oleh peraturan perundang-undangan setempat, bukti validasi identitas, dan pemeriksaan tambahan apa pun yang dianggap

1.4 Supplier will provide security and privacy education to its employees annually and require all such employees to certify each year that they will comply with Supplier's ethical business conduct, confidentiality, and security policies, as set out in Supplier's code of conduct or similar documents. Supplier will provide additional policy and process training to persons with administrative access to any components of the Services, Deliverables or Kyndryl Materials, with such training specific to their role and support of the Services, Deliverables and Kyndryl Materials, and as necessary to maintain required compliance and certifications.

1.5 Supplier will design security and privacy measures to protect and maintain the availability of Kyndryl Materials, including through its implementation, maintenance, and compliance with policies and procedures which require security and privacy by design, secure engineering, and secure operations, for all Services and Deliverables and for all Handling of Kyndryl Technology.

2. Security Incidents

2.1 Supplier will maintain and follow documented incident response policies consistent with Industry Best Practices for computer security incident handling.

2.2 Supplier will investigate unauthorized access or unauthorized use of Kyndryl Materials and will define and execute an appropriate response plan.

2.3 Supplier will promptly (and in no event any later than 48 hours) notify Kyndryl after becoming aware of any Security Breach. Supplier will provide such notification to cyber.incidents@kyndryl.com. Supplier will provide Kyndryl with reasonably requested information about such breach and the status of any Supplier remediation and restoration activities. By way of example, reasonably requested information may include logs demonstrating privileged, administrative, and other access to Devices, systems or applications, forensic images of Devices, systems or applications, and other similar items, to the extent relevant to the breach or Supplier's remediation and restoration activities.

penting oleh Pemasok. Pemasok akan secara berkala mengulang dan memvalidasi ulang persyaratan ini karena hal ini dianggap penting.

1.4 Pemasok akan memberikan pendidikan keamanan dan kerahasiaan setiap tahun kepada karyawannya dan mewajibkan semua karyawan tersebut untuk menjamin setiap tahunnya bahwa mereka akan mematuhi kode etik bisnis, kerahasiaan, dan kebijakan keamanan Pemasok, sebagaimana yang diatur dalam kode etik Pemasok atau dokumen serupa. Pemasok akan memberikan pelatihan kebijakan dan proses tambahan kepada orang-orang dengan akses administratif ke setiap komponen Layanan, Materi yang Disampaikan atau Materi Kyndryl, dengan pelatihan semacam itu khusus untuk peran dan dukungan mereka pada Layanan, Materi yang Disampaikan, dan Materi Kyndryl, dan sebagaimana yang diperlukan untuk mempertahankan kepatuhan dan sertifikasi yang diwajibkan.

1.5 Pemasok akan merancang tindakan keamanan dan kerahasiaan untuk melindungi dan mengelola ketersediaan Materi Kyndryl, termasuk melalui implementasi, pemeliharaan, dan kepatuhannya terhadap kebijakan dan prosedur yang memerlukan keamanan dan kerahasiaan berdasarkan rancangan, rekayasa aman, dan operasi yang aman, untuk semua Layanan dan Materi yang Disampaikan dan untuk semua Penanganan Teknologi Kyndryl.

2. Insiden Keamanan

2.1 Pemasok akan mempertahankan dan mengikuti kebijakan tanggapan insiden yang didokumentasikan sesuai dengan Praktik Terbaik Industri untuk penanganan insiden keamanan komputer.

2.2 Pemasok akan menginvestigasi akses yang tidak sah atau penggunaan yang sah atas Materi Kyndryl dan akan menentukan dan melaksanakan rencana tanggapan yang sesuai.

2.3 Pemasok akan segera (dan tidak lebih dari 48 jam) memberi tahu Kyndryl setelah mengetahui adanya Pelanggaran Keamanan. Pemasok akan memberikan pemberitahuan seperti ke cyber.incidents@kyndryl.com. Pemasok akan memberikan informasi yang diminta secara wajar kepada Kyndryl mengenai pelanggaran tersebut dan status setiap aktivitas perbaikan dan restorasi Pemasok. Sebagai contoh, informasi yang diminta secara wajar dapat mencakup log yang mendemonstrasikan akses istimewa, administratif, dan akses lain ke Perangkat, sistem atau aplikasi, gambar forensik Perangkat, sistem atau aplikasi, dan

2.4 Supplier will provide Kyndryl with reasonable assistance to satisfy any legal obligations (including obligations to notify regulators or Data Subjects) of Kyndryl, Kyndryl affiliates and Customers (and their customers and affiliates) in relation to a Security Breach.

2.5 Supplier will not inform or notify any third party that a Security Breach directly or indirectly relates to Kyndryl or Kyndryl Materials unless Kyndryl approves doing so in writing or where required by law. Supplier will notify Kyndryl in writing prior to distributing any legally required notification to any third-party, where the notification would directly or indirectly reveal Kyndryl's identity.

2.6 In case of a Security Breach which arises from Supplier's breach of any obligation under these Terms:

(a) Supplier will be responsible for any costs it incurs, as well as actual costs that Kyndryl incurs, in providing notification of the Security Breach to applicable regulators, other government and relevant industry self-regulatory agencies, the media (if required by applicable law), Data Subjects, Customers, and others,

(b) if Kyndryl requests, Supplier will establish and maintain at Supplier's own expense a call-center to respond to questions from Data Subjects about the Security Breach and its consequences, for 1 year after the date on which such Data Subjects were notified of the Security Breach, or as required by any applicable data protection law, whichever affords greater protection. Kyndryl and Supplier will work together to create the scripts and other materials to be used by call-center staff when responding to inquiries. Alternatively, on written notice to Supplier, Kyndryl may establish and maintain its own call-center, in lieu of having Supplier establish a call-center, and Supplier will reimburse Kyndryl the actual costs that Kyndryl incurs in establishing and maintaining such call-center, and

item serupa lainnya, sejauh relevan dengan pelanggaran atau aktivitas perbaikan dan restorasi Pemasok.

2.4 Pemasok akan memberikan bantuan yang wajar kepada Kyndryl untuk memenuhi setiap kewajiban hukum apa pun (termasuk kebijakan untuk memberi tahu pembuat peraturan atau Subjek Data) Kyndryl, afiliasi Kyndryl dan Pelanggan (dan pelanggan serta afiliasi mereka) berkaitan dengan Pelanggaran Keamanan.

2.5 Pemasok tidak akan menginformasikan atau memberi tahu pihak ketiga mana pun bahwa Pelanggaran Keamanan secara langsung atau tidak langsung berkaitan dengan Kyndryl atau Materi Kyndryl kecuali jika Kyndryl menyetujuinya secara tertulis atau jika diwajibkan oleh hukum. Pemasok akan memberi tahu Kyndryl secara tertulis sebelum mendistribusikan setiap pemberitahuan yang diwajibkan secara hukum kepada pihak ketiga mana pun, jika pemberitahuan akan secara langsung atau tidak langsung mengungkap identitas Kyndryl.

2.6 Dalam hal Pelanggaran Keamanan yang timbul dari pelanggaran Pemasok terhadap kewajiban apa pun berdasarkan Syarat-Syarat ini:

(a) Pemasok akan bertanggung jawab atas setiap biaya yang dikeluarkan olehnya, serta biaya aktual yang dikeluarkan oleh Kyndryl, dalam memberikan pemberitahuan tentang Pelanggaran Keamanan kepada pembuat peraturan yang berlaku, badan pemerintah dan lembaga pengatur mandiri industri terkait lainnya, media (jika diwajibkan oleh hukum yang berlaku), Subjek Data, Pelanggan, dan pihak lainnya,

(b) apabila Kyndryl meminta, Pemasok akan membangun dan mengelola pusat panggilan dengan biaya yang ditanggung oleh Pemasok sendiri untuk menanggapi pertanyaan dari Subjek Data tentang Pelanggaran Keamanan dan konsekuensinya, selama 1 tahun setelah tanggal saat Subjek Data tersebut diberi tahu tentang Pelanggaran Keamanan, atau sebagaimana yang diwajibkan oleh hukum perlindungan data yang berlaku, mana pun yang memberikan perlindungan lebih besar. Kyndryl dan Pemasok akan bekerja sama untuk membuat skrip dan materi lain yang digunakan oleh staf pusat panggilan saat menanggapi pertanyaan. Atau, dengan pemberitahuan tertulis kepada Pemasok, Kyndryl dapat membangun dan mengelola pusat panggilannya sendiri, sebagai pengganti meminta Pemasok

(c) Supplier will reimburse Kyndryl the actual costs that Kyndryl incurs in providing credit monitoring and credit restoration services for 1 year after the date on which individuals affected by the breach who choose to register for such services were notified of the Security Breach, or as required by any applicable data protection law, whichever affords greater protection.

3. Physical Security and Entry Control (as used below, "Facility" means a physical location where Supplier hosts, processes or otherwise accesses Kyndryl Materials).

3.1 Supplier will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into Facilities.

3.2 Supplier will require authorized approval for access to Facilities and controlled areas within Facilities, including any temporary access, and will limit access by job role and business need. If Supplier grants temporary access, its authorized employee will escort any visitor while in the Facility and any controlled areas.

3.3 Supplier will implement physical access controls, including multi-factor access controls that are consistent with Industry Best Practices, to appropriately restrict entrance to controlled areas within Facilities, will log all entry attempts, and retain such logs for at least one year.

3.4 Supplier will revoke access to Facilities and controlled areas within Facilities upon (a) separation of an authorized Supplier employee or (b) the authorized Supplier employee no longer having a valid business need for access. Supplier will follow formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.

3.5 Supplier will take precautions to protect all physical infrastructure used to support the Services and Deliverables and the Handling of Kyndryl

membangun pusat panggilan, dan Pemasok akan mengganti biaya kepada Kyndryl atas biaya aktual yang dikeluarkan oleh Kyndryl dalam membangun dan mengelola pusat panggilan tersebut, dan

(c) Pemasok akan mengganti biaya kepada Kyndryl atas biaya aktual yang dikeluarkan oleh Kyndryl dalam memberikan layanan pemantauan kredit dan restorasi kredit selama 1 tahun setelah tanggal saat individu yang terdampak oleh pelanggaran yang memilih untuk mendaftar layanan tersebut diberi tahu tentang Pelanggaran Keamanan, atau sebagaimana yang diwajibkan oleh setiap hukum perlindungan data yang berlaku, mana pun yang memberikan perlindungan lebih besar.

3. Kontrol Entri dan Keamanan Fisik (sebagaimana yang digunakan di bawah ini, "Fasilitas" berarti lokasi fisik di mana Pemasok menyelenggarakan, memproses atau mengakses Materi Kyndryl).

3.1 Pemasok akan mempertahankan kontrol entri fisik yang sesuai seperti penghalang, titik entri yang dikendalikan kartu, kamera pengawas, dan orang di bagian penerimaan untuk melindungi dari entri yang tidak sah ke dalam Fasilitas.

3.2 Pemasok akan memerlukan persetujuan yang sah untuk akses ke Fasilitas dan area yang dikontrol dalam Fasilitas, termasuk setiap akses sementara, dan akan membatasi akses menurut peran pekerjaan dan keperluan bisnis. Apabila Pemasok memberikan akses sementara, karyawannya yang sah akan mengantar setiap pengunjung saat berada di Fasilitas dan setiap area yang dikontrol.

3.3 Pemasok akan mengimplementasikan kontrol akses fisik, termasuk kontrol akses multifaktor yang sesuai dengan Praktik Terbaik Industri, guna membatasi secara tepat pintu masuk ke area yang dikontrol dalam Fasilitas, akan mencatat semua upaya masuk, dan menyimpan log tersebut selama setidaknya satu tahun.

3.4 Pemasok akan mencabut akses ke Fasilitas dan area yang dikontrol dalam Fasilitas setelah (a) pemisahan karyawan Pemasok yang sah atau (b) karyawan Pemasok yang sah tidak lagi memiliki kebutuhan bisnis yang valid untuk akses. Pemasok akan mengikuti prosedur pemisahan formal yang didokumentasikan yang mencakup penghapusan cepat dari daftar kontrol akses dan penyerahan tanda pengenal akses fisik.

3.5 Pemasok akan melakukan tindakan pencegahan untuk melindungi semua infrastruktur

Technology against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

4. Access, Intervention, Transfer, and Separation Control

4.1 Supplier will maintain documented security architecture of networks that it manages in its operation of the Services, its provision of Deliverables and its Handling of Kyndryl Technology. Supplier will separately review such network architecture, and employ measures to prevent unauthorized network connections to systems, applications, and network devices, for compliance with secure segmentation, isolation, and defense in-depth standards. Supplier may not use wireless technology in its hosting and operations of any Hosted Services; otherwise, Supplier may use wireless networking technology in its delivery of Services and Deliverables and in its Handing of Kyndryl Technology, but Supplier will encrypt and require secure authentication for any such wireless networks.

4.2 Supplier will maintain measures that are designed to logically separate and prevent Kyndryl Materials from being exposed to or accessed by unauthorized persons. Further, Supplier will maintain appropriate isolation of its production, non-production, and other environments, and, if Kyndryl Materials are already present within or are transferred to a non-production environment (for example to reproduce an error), then Supplier will ensure that the security and privacy protections in the non-production environment are equal to those in the production environment.

4.3 Supplier will encrypt Kyndryl Materials in transit and at rest (unless Supplier demonstrates to Kyndryl's reasonable satisfaction that encrypting Kyndryl Materials at rest is technically infeasible). Supplier will also encrypt all physical media, if any, such as media containing backup files. Supplier will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use associated with data encryption. Supplier will ensure that the specific cryptographic methods used for such encryption align with Industry Best Practices (such as NIST SP 800-131a).

fisik yang digunakan untuk mendukung Layanan dan Materi yang Disampaikan dan Penanganan Teknologi Kyndryl terhadap ancaman lingkungan, baik yang ditimbulkan oleh alam atau manusia, seperti temperatur sekitar yang berlebih, kebakaran, banjir, kelembapan, pencurian, dan vandalisme.

4. Akses, Intervensi, Transfer, dan Kontrol Pemisahan

4.1 Pemasok akan memelihara arsitektur keamanan jaringan yang didokumentasi yang dikelolanya dalam pengoperasiannya atas Layanan, penyediaannya atas Materi yang Disampaikan, dan Penanganannya atas Teknologi Kyndryl. Pemasok akan meninjau arsitektur jaringan tersebut secara terpisah, dan menggunakan tindakan-tindakan untuk mencegah koneksi jaringan yang tidak sah ke sistem, aplikasi, dan perangkat jaringan, memastikan kepatuhan dengan segmentasi yang aman, isolasi, dan standar pertahanan yang mendalam. Pemasok tidak dapat menggunakan teknologi nirkabel dalam hosting dan operasinya dari setiap Layanan yang Di-Host; atau, Pemasok dapat menggunakan teknologi jaringan nirkabel dalam penyampaian Layanan dan Materi yang Disampaikan dan Penanganan Teknologi Kyndryl, tetapi Pemasok akan mengenkripsi dan mewajibkan autentikasi aman untuk setiap jaringan nirkabel tersebut.

4.2 Pemasok akan mempertahankan tindakan-tindakan yang dirancang untuk secara logis memisahkan dan mencegah Materi Kyndryl diekspos ke atau diakses oleh orang yang tidak sah. Selanjutnya, Pemasok akan memelihara isolasi yang tepat dari produksi, non-produksi, dan lingkungan apa pun lainnya, dan, jika Materi Kyndryl telah ada atau ditransfer ke lingkungan non-produksi (misalnya untuk mereproduksi kesalahan), maka Pemasok akan memastikan bahwa perlindungan keamanan dan kerahasiaan dalam lingkungan non-produksi setara dengan perlindungan dalam lingkungan produksi.

4.3 Pemasok akan mengenkripsi Materi Kyndryl di dalam jaringan (in transit) dan saat berada di penyimpanan (at rest) (kecuali apabila Pemasok mendemonstrasikan pada kepuasan Kyndryl yang wajar bahwa mengenkripsi Materi Kyndryl saat berada di penyimpanan secara teknis tidak layak). Pemasok juga akan mengenkripsi semua media fisik, jika ada, seperti media yang berisi file cadangan. Pemasok akan mempertahankan prosedur yang didokumentasikan untuk pembuatan, penerbitan, distribusi, penyimpanan, putaran, penangguhan, pemulihan, pencadangan, pemusnahan, akses, dan penggunaan kunci yang aman terkait dengan enkripsi

data. Pemasok akan memastikan bahwa metode kriptografis khusus yang digunakan untuk enkripsi tersebut diselaraskan dengan Praktik Terbaik Industri (seperti NIST SP 800-131a).

4.4 If Supplier requires access to Kyndryl Materials, Supplier will restrict and limit such access to the least level required to provide and support the Services and Deliverables. Supplier will require that such access, including administrative access to any underlying components (i.e., privileged access), will be individual, role based, and subject to approval and regular validation by authorized Supplier employees following segregation of duty principles. Supplier will maintain measures to identify and remove redundant and dormant accounts. Supplier will also revoke accounts with privileged access within twenty-four (24) hours after the account owner's separation or the request by Kyndryl or any authorized Supplier employee, such as the account owner's manager.

4.4 Apabila Pemasok memerlukan akses ke Materi Kyndryl, Pemasok akan memperketat dan membatasi akses tersebut ke tingkat terendah yang diperlukan untuk memberikan dan mendukung Layanan dan Materi yang Disampaikan. Pemasok akan mewajibkan bahwa akses tersebut, termasuk akses administratif ke setiap komponen dasar (yaitu, akses khusus), akan berdiri sendiri, berbasis peran, dan tunduk pada persetujuan dan validasi rutin oleh karyawan Pemasok yang berwenang setelah pemisahan prinsip kewajiban. Pemasok akan mempertahankan tindakan untuk mengidentifikasi dan menghapus akun redundan dan dorman. Pemasok juga akan mencabut akun dengan hak istimewa dalam dua puluh empat (24) jam setelah pemisahan pemilik akun atau permintaan oleh Kyndryl atau setiap karyawan Pemasok yang sah, seperti manajer pemilik akun.

4.5 Consistent with Industry Best Practices, Supplier will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases. Additionally, Supplier will utilize multi-factor authentication for all non-console based privileged access to any Kyndryl Materials.

4.5 Sesuai dengan Praktik Terbaik Industri, Pemasok akan mempertahankan tindakan teknis yang menerapkan batas waktu sesi tidak aktif, penguncian akun setelah beberapa upaya login gagal secara berurutan, autentikasi kata sandi atau frasa sandi yang kuat, dan tindakan yang memerlukan transfer dan penyimpanan kata sandi dan frasa sandi tersebut dengan aman. Selain itu, Pemasok akan menggunakan autentikasi multifaktor untuk semua akses istimewa berbasis non-konsol ke Materi Kyndryl apa pun.

4.6 Supplier will monitor use of privileged access and maintain security information and event management measures designed to: (a) identify unauthorized access and activity, (b) facilitate a timely and appropriate response to such access and activity, and (c) enable audits by Supplier, Kyndryl (pursuant to its verification rights in these Terms and audit rights in the Transaction Document or associated base or other related agreement between the parties) and others of compliance with documented Supplier policy.

4.6 Pemasok akan memantau penggunaan akses istimewa dan mempertahankan tindakan informasi keamanan dan manajemen peristiwa yang dirancang untuk: (a) mengidentifikasi akses dan aktivitas yang tidak sah, (b) memfasilitasi tanggapan yang tepat waktu dan sesuai ke akses dan aktivitas tersebut, dan (c) memungkinkan audit oleh Pemasok, Kyndryl (menurut hak verifikasinya dalam Syarat-Syarat dan hak audit dalam Dokumen Transaksi atau perjanjian dasar terkait atau perjanjian lainnya yang terkait di antara para pihak) dan kepatuhan lainnya dengan kebijakan Pemasok yang didokumentasikan.

4.7 Supplier will retain logs in which it records, in compliance with Industry Best Practices, all administrative, user, or other access or activity to or with respect to systems used in providing Services or Deliverables and in Handling Kyndryl Technology (and will provide those logs to Kyndryl upon request). Supplier will maintain measures designed to protect against unauthorized access, modification,

4.7 Pemasok akan menyimpan log yang mencatat, dengan mematuhi Praktik Terbaik Industri, semua akses administratif, pengguna, atau aktivitas ke atau berkenaan dengan sistem yang digunakan dalam memberikan Layanan atau Materi yang Disampaikan dan dalam Penanganan Teknologi Kyndryl (dan akan memberikan log tersebut kepada

and accidental or deliberate destruction of such logs.

4.8 Supplier will maintain computing protections for systems that it owns or manages, including end-user systems, and that it uses in providing Services or Deliverables or in Handling Kyndryl Technology, with such protections including: endpoint firewalls, full disk encryption, signature and non-signature based endpoint detection and response technologies to address malware and advanced persistent threats, time based screen locks, and endpoint management solutions that enforce security configuration and patching requirements. In addition, Supplier will implement technical and operational controls that ensure only known and trusted end-user systems are allowed to use Supplier networks.

4.9 Consistent with Industry Best Practices, Supplier will maintain protections for data center environments where Kyndryl Material are present or processed, with such protections including intrusion detection and prevention and denial of service attack countermeasures and mitigation.

5. Service and Systems Integrity and Availability Control

5.1 Supplier will: (a) perform security and privacy risk assessments at least annually, (b) perform security testing and assess vulnerabilities, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter as it concerns Services and Deliverables and annually with respect to its Handling of Kyndryl Technology, (c) enlist a qualified independent third-party to perform penetration testing consistent with Industry Best Practices at least annually, with such testing including both automated and manual testing, (d) perform automated management and routine verification of compliance with security configuration requirements for each component of the Services and Deliverables and with respect to its Handling of Kyndryl Technology, and (e) remediate identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact. Supplier will take reasonable steps to avoid disruption of Services when performing its tests, assessments, scans, and execution of remediation activities. Upon Kyndryl's

Kyndryl atas permintaan). Pemasok akan mempertahankan tindakan yang dirancang untuk melindungi terhadap akses yang tidak sah, modifikasi, dan pemusnahan atas log tersebut secara sengaja atau tidak disengaja.

4.8 Pemasok akan mempertahankan perlindungan komputasi untuk sistem yang dimiliki atau dikelola Pemasok, termasuk sistem pengguna akhir, dan yang digunakan dalam menyediakan Layanan atau Materi yang Disampaikan atau dalam Penanganan Teknologi Kyndryl, dengan perlindungan tersebut termasuk: firewall titik akhir, enkripsi disk penuh, teknologi deteksi dan tanggapan titik akhir berbasis tanda tangan dan non-tanda tangan untuk mengatasi ancaman malware dan ancaman persisten tingkat lanjut, kunci layar berbasis waktu, dan solusi manajemen titik akhir yang menerapkan persyaratan konfigurasi dan patching keamanan. Selain itu, Pemasok akan mengimplementasikan kontrol teknis dan operasional yang memastikan hanya sistem pengguna akhir yang diketahui dan tepercaya yang diizinkan untuk menggunakan jaringan Pemasok.

4.9 Sesuai dengan Praktik Terbaik Industri, Pemasok akan mempertahankan perlindungan untuk lingkungan pusat data di mana Materi Kyndryl diberikan atau diproses, dengan perlindungan tersebut yang mencakup deteksi dan pencegahan intrusi dan penolakan penanggulangan serangan layanan dan mitigasi.

5. Integritas Layanan dan Sistem dan Kontrol Ketersediaan

5.1 Pemasok akan: (a) menjalankan penilaian risiko keamanan dan kerahasiaan setidaknya setiap tahun, (b) menjalankan pengujian keamanan dan menilai kerentanan, termasuk pemindaian sistem otomatis dan keamanan aplikasi serta peretasan etika manual, sebelum rilis produksi dan setiap tahun setelahnya sebagaimana menyangkut Layanan dan Materi yang Disampaikan dan setiap tahun sehubungan dengan Penanganan Teknologi Kyndryl, (c) menyertakan pihak ketiga independen yang memenuhi syarat untuk menjalankan pengujian penetrasi sesuai dengan Praktik Terbaik Industri setidaknya setiap tahun, dengan pengujian tersebut meliputi pengujian otomatis dan manual, (d) menjalankan manajemen otomatis dan verifikasi kepatuhan rutin dengan persyaratan konfigurasi keamanan untuk masing-masing komponen Layanan dan Materi yang Disampaikan dan berkenaan dengan Penanganan Teknologi Kyndryl, dan (e) memperbaiki kerentanan yang diidentifikasi atau

request, Supplier will provide Kyndryl with a written summary of Supplier's then-most recent penetration testing activities, which report will at a minimum include the name of the offerings covered by the testing, the number of systems or applications in-scope for the testing, the dates of the testing, the methodology used in the testing, and a high-level summary of findings.

5.2 Supplier will maintain policies and procedures designed to manage risks associated with the application of changes to the Services or Deliverables or to the Handling of Kyndryl Technology. Prior to implementing such a change, including to affected systems, networks, and underlying components, Supplier will document in a registered change request: (a) a description of and reason for the change, (b) implementation details and schedule, (c) a risk statement addressing impact to the Services and Deliverables, customers of the Services, or Kyndryl Materials, (d) expected outcome, (e) rollback plan, and (f) approval by authorized Supplier employees.

5.3 Supplier will maintain an inventory of all IT assets it uses in operating the Services, providing Deliverables and in Handling Kyndryl Technology. Supplier will continuously monitor and manage the health (including capacity) and availability of such IT assets, Services, Deliverables and Kyndryl Technology, including the underlying components of such assets, Services, Deliverables and Kyndryl Technology.

5.4 Supplier will build all systems that it uses in the development or operation of Services and Deliverables and in its Handling of Kyndryl Technology from predefined system security images or security baselines, which satisfy Industry Best Practices, such as the Center for Internet Security (CIS) benchmarks.

5.5 Without limiting Supplier's obligations or Kyndryl's rights under the Transaction Document or associated base agreement between the parties with respect to business continuity, Supplier will

ketidakpatuhan dengan persyaratan konfigurasi keamanan berdasarkan risiko yang berkaitan, eksploitabilitas, dan dampak. Pemasok akan mengambil langkah yang wajar guna menghindari gangguan Layanan saat menjalankan pengujian, penilaian, pemindaian, dan pelaksanaannya atas aktivitas perbaikan. Atas permintaan Kyndryl, Pemasok akan memberikan kepada Kyndryl ringkasan tertulis dari aktivitas pengujian penetrasi terbaru Pemasok pada saat itu, laporan mana yang akan menyertakan setidaknya nama tawaran yang dicakup oleh pengujian, jumlah sistem atau aplikasi dalam cakupan untuk pengujian, tanggal pengujian, metodologi yang digunakan dalam pengujian, dan ringkasan temuan tingkat tinggi.

5.2 Pemasok akan mempertahankan kebijakan dan prosedur yang dirancang untuk mengelola risiko yang terkait dengan penerapan perubahan terhadap Layanan atau Materi yang Disampaikan atau Penanganan Teknologi Kyndryl. Sebelum mengimplementasikan perubahan apa pun, termasuk sistem, jaringan, dan komponen dasar yang terkena dampak, Pemasok akan mendokumentasikan dalam permintaan perubahan terdaftar: (a) uraian dan alasan untuk perubahan, (b) rincian implementasi dan jadwal, (c) pernyataan risiko mengenai pengaruh pada Layanan dan Materi yang Disampaikan, pelanggan Layanan, atau Materi Kyndryl, (d) hasil yang diharapkan, (e) rencana pengembalian, dan (f) persetujuan oleh karyawan Pemasok yang sah.

5.3 Pemasok akan memelihara inventaris dari semua aset TI yang pihaknya gunakan dalam pengoperasian Layanan, yang menyediakan Materi yang Disampaikan dan Penanganan Teknologi Kyndryl. Pemasok akan terus memantau dan mengelola kondisi (termasuk kapasitas) dan ketersediaan aset IT tersebut, Layanan, Materi yang Disampaikan, dan Teknologi Kyndryl, termasuk komponen dasar dari aset, Layanan, Materi yang Disampaikan, dan Teknologi Kyndryl tersebut.

5.4 Pemasok akan mendirikan semua sistem yang pihaknya gunakan dalam pengembangan atau operasi Layanan dan Materi yang Disampaikan dan Penanganan Teknologi Kyndryl dari gambar keamanan sistem atau garis dasar keamanan yang telah ditentukan sebelumnya, yang memenuhi Praktik Terbaik Industri, seperti tolok ukur Center for Internet Security (CIS).

5.5 Tanpa membatasi kewajiban Pemasok atau hak-hak Kyndryl berdasarkan Dokumen Transaksi atau perjanjian dasar yang terkait di antara para pihak sehubungan dengan kesinambungan bisnis, Pemasok

separately assess each Service and Deliverable and each IT system used in Handling Kyndryl Technology for business and IT continuity and disaster recovery requirements pursuant to documented risk management guidelines. Supplier will ensure that each such Service, Deliverable and IT system has, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business and IT continuity and disaster recovery plans consistent with Industry Best Practices. Supplier will ensure that such plans are designed to deliver the specific recovery times that are set forth in Section 5.6 below.

akan menilai secara terpisah setiap Layanan dan Materi yang Disampaikan dan masing-masing sistem TI yang digunakan dalam Penanganan Teknologi Kyndryl untuk bisnis dan kesinambungan TI serta persyaratan pemulihan bencana sesuai dengan pedoman manajemen risiko yang didokumentasikan. Pemasok akan memastikan bahwa setiap Layanan, Materi yang Disampaikan, dan sistem TI telah, sejauh dijamin oleh penilaian risiko tersebut, secara terpisah menentukan, mendokumentasikan, memelihara, dan setiap tahun memvalidasi rencana pemulihan bencana dan kesinambungan TI dan bisnis sesuai dengan Praktik Terbaik Industri. Pemasok akan memastikan bahwa rencana tersebut dirancang untuk menyampaikan waktu pemulihan spesifik yang tercantum dalam Bagian 5.6 di bawah ini.

5.6 The specific recovery point objectives ("**RPO**") and recovery time objectives ("**RTO**") with respect to any Hosted Service are: 24 hours RPO and 24 hours RTO; nevertheless, Supplier will comply with any shorter duration RPO or RTO that Kyndryl has committed to a Customer, promptly after Kyndryl notifies Supplier in writing of such shorter duration RPO or RTO (an email constitutes a writing). As it concerns all other Services provided by Supplier to Kyndryl, Supplier will ensure that its business continuity and disaster recovery plans are designed to deliver RPO and RTO that enable Supplier to remain in compliance with all of its obligations to Kyndryl under the Transaction Document and associated base agreement between the parties, and these Terms, including its obligations to timely provide testing, support, and maintenance.

5.6 Sasaran titik pemulihan (recovery point objectives - "**RPO**") dan sasaran waktu pemilihan (recovery time objectives - "**RTO**") spesifik sehubungan dengan setiap Layanan yang Di-Host adalah: 24 jam RPO dan 24 jam RTO; meski demikian, Pemasok akan mematuhi setiap durasi RPO atau RTO yang lebih pendek yang telah menjadi komitmen Kyndryl kepada Pelanggan, segera setelah Kyndryl memberi tahu Pemasok secara tertulis mengenai durasi RPO atau RTO yang lebih pendek (email juga dianggap sebagai pernyataan tertulis). Karena menyangkut semua Layanan lain yang diberikan oleh Pemasok kepada Kyndryl, Pemasok akan memastikan bahwa rencana pemulihan bencana dan kesinambungan bisnisnya dirancang untuk menyampaikan RPO dan RTO yang memungkinkan Pemasok untuk tetap mematuhi semua kewajibannya kepada Kyndryl berdasarkan Dokumen Transaksi dan perjanjian dasar terkait di antara para pihak, dan Syarat-Syarat ini, termasuk kewajibannya untuk memberikan pengujian, dukungan, dan pemeliharaan secara tepat waktu.

5.7 Supplier will maintain measures designed to assess, test, and apply security advisory patches to the Services and Deliverables and associated systems, networks, applications, and underlying components within the scope of those Services and Deliverables, as well as the systems, networks, applications, and underlying components used to Handle Kyndryl Technology. Upon determining that a security advisory patch is applicable and appropriate, Supplier will implement the patch pursuant to documented severity and risk assessment guidelines. Supplier's implementation of security advisory patches will be subject to its change management policy.

5.7 Pemasok akan mempertahankan tindakan yang dirancang untuk menilai, menguji, dan menerapkan patch saran keamanan untuk Layanan dan Materi yang Disampaikan dan sistem, jaringan, aplikasi, dan komponen dasar terkait dalam cakupan Layanan dan Materi yang Disampaikan tersebut, serta sistem, jaringan, aplikasi, dan komponen dasar yang digunakan untuk Penanganan Teknologi Kyndryl. Setelah menentukan bahwa patch saran keamanan berlaku dan sesuai, Pemasok akan mengimplementasikan patch sesuai dengan pedoman tingkat permasalahan dan penilaian risiko yang didokumentasikan. Implementasi patch saran

5.8 If Kyndryl has a reasonable basis for believing that hardware or software that Supplier provides to Kyndryl may contain intrusive elements, such as spyware, malware, or malicious code, then Supplier will timely cooperate with Kyndryl in investigating and remediating Kyndryl's concerns.

6. Service Provisioning

6.1 Supplier will support industry common methods of federated authentication for any Kyndryl user or Customer accounts, with Supplier following Industry Best Practices in authenticating such Kyndryl user or Customer accounts (such as by Kyndryl centrally managed multi-factor Single Sign-On, using OpenID Connect or Security Assertion Markup Language).

7. Subcontractors. Without limiting Supplier's obligations or Kyndryl's rights under the Transaction Document or associated base agreement between the parties with respect to the retention of subcontractors, Supplier will ensure that any subcontractor performing work for Supplier has instituted governance controls to comply with the requirements and obligations that these Terms place on Supplier.

8. Physical Media. Supplier will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with Industry Best Practices for media sanitization.

keamanan oleh Pemasok akan tunduk pada kebijakan manajemen perubahannya.

5.8 Jika Kyndryl memiliki dasar yang wajar untuk meyakini bahwa perangkat keras atau perangkat lunak yang disediakan oleh Pemasok kepada Kyndryl mungkin berisi elemen intrusif, seperti spyware, malware, atau kode berbahaya, Pemasok akan bekerja sama dengan Kyndryl secara tepat waktu dalam investigasi dan perbaikan persoalan Kyndryl.

6. Penyediaan Layanan

6.1 Pemasok akan mendukung metode autentikasi terfederasi yang umum dalam industri untuk setiap akun Pelanggan atau pengguna Kyndryl, dengan Pemasok yang mengikuti Praktik Terbaik Industri dalam mengautentikasi akun Pelanggan atau pengguna Kyndryl tersebut (seperti Single Sign-On multifaktor yang dikelola Kyndryl secara terpusat, menggunakan OpenID Connect atau Security Assertion Markup Language).

7. Subkontraktor. Tanpa membatasi kewajiban Pemasok atau hak-hak Kyndryl berdasarkan Dokumen Transaksi atau perjanjian dasar yang terkait di antara para pihak sehubungan dengan retensi subkontraktor, Pemasok akan memastikan bahwa setiap subkontraktor yang menjalankan pekerjaan untuk Pemasok telah memulai kontrol tata kelola untuk mematuhi persyaratan dan kewajiban yang dikenakan oleh Syarat-Syarat ini kepada Pemasok.

8. Media Fisik. Pemasok akan membersihkan media fisik yang ditujukan untuk penggunaan ulang dengan aman sebelum penggunaan ulang tersebut dan akan memusnahkan media fisik yang tidak ditujukan untuk penggunaan ulang, sesuai dengan Praktik Terbaik Industri untuk pembersihan media.

Article IX, Hosted Services' Certifications and Reports

This Article applies if Supplier provides a Hosted Service to Kyndryl.

1.1 Supplier will obtain the following certifications or reports within the time frames set forth below:

Pasal IX, Sertifikasi dan Laporan Layanan yang Di-Host

Pasal ini berlaku jika Pemasok menyediakan Layanan yang Di-Host kepada Kyndryl.

1.1 Pemasok akan mendapatkan sertifikasi atau laporan berikut dalam kerangka waktu yang dicantumkan di bawah ini:

Certifications / Reports/ ***Sertifikasi / Laporan***	**Time Frame/** ***Kerangka Waktu***
With respect to Supplier's Hosted Services:/ ***Berkenaan dengan Layanan yang Di-Host Pemasok:*** Certification of compliance with ISO 27001, Information technology, Security techniques, Information security management systems, with such certification based on the assessment of a reputable independent auditor/ *Sertifikasi kepatuhan dengan ISO 27001, Teknologi informasi, Teknik keamanan, Sistem manajemen keamanan informasi, dengan sertifikasi yang didasarkan pada penilaian auditor independen yang bereputasi* **Or/** ***Atau*** SOC 2 Type 2: A report by a reputable independent auditor demonstrating its review of Supplier's systems, controls and operations in accordance with a SOC 2 Type 2 (including, at a minimum, security, confidentiality, and availability)/ *SOC 2 Tipe 2: Laporan oleh auditor independen bereputasi yang mendemonstrasikan tinjauannya tentang sistem, kontrol, dan operasi Pemasok sesuai dengan SOC 2 Tipe 2 (termasuk minimum keamanan, kerahasiaan, dan ketersediaan)*	Supplier will obtain the ISO 27001 certification by 120 Days after the effective date of the Transaction Document* or Assumption Date** and then renew the certification based on the assessment of a reputable independent auditor every 12 months thereafter (with each renewal against the then most current version of the standard)/ *Pemasok akan memperoleh sertifikasi ISO 27001 pada 120 hari setelah tanggal mulai berlaku Dokumen Transaksi ini* atau Tanggal Asumsi** dan kemudian memperbarui sertifikasi berdasarkan penilaian auditor independen bereputasi setiap 12 bulan setelahnya (dengan masing-masing pembaruan terhadap versi standar paling baru saat itu)* Supplier will obtain the SOC 2 Type 2 report by 240 Days after the effective date of the Transaction Document* or Assumption Date** and then obtain a new report by a reputable independent auditor demonstrating its review of Supplier's systems, controls and operations in accordance with a SOC 2 Type 2 (including, at a minimum, security, confidentiality, and availability) every 12 months thereafter/ *Pemasok akan memperoleh laporan SOC 2 Tipe 2 paling lambat 240 Hari setelah tanggal mulai berlaku Dokumen Transaksi* atau Tanggal Asumsi** dan kemudian memperoleh laporan baru oleh auditor independen bereputasi yang mendemonstrasikan tinjauannya atas sistem, kontrol, dan operasi Pemasok sesuai dengan SOC 2 Tipe 2 (termasuk, minimal, keamanan, kerahasiaan, dan ketersediaan) setiap 12 bulan setelahnya* * If, as of such effective date, Supplier provides a Hosted Service/ *Apabila, pada tanggal mulai berlaku, Pemasok memberikan Layanan yang Di-Host* ** The date that Supplier assumes an obligation to provide a Hosted Service/ *Tanggal ketika Pemasok menanggung kewajiban untuk menyediakan Layanan yang Di-Host*

1.2 If Supplier requests in writing, and Kyndryl approves in writing, Supplier may obtain a substantially equivalent certification or report to those referenced above, with the understanding that the time frames set forth in the table above would apply unchanged with respect to the substantially equivalent certification or report.

1.2 Jika Pemasok meminta secara tertulis, dan Kyndryl menyetujui secara tertulis, Pemasok dapat memperoleh sertifikasi atau laporan yang setara secara substansial ke referensi di atas, dengan pemahaman bahwa kerangka waktu yang tercantum dalam tabel di atas akan berlaku tanpa perubahan berkenaan dengan sertifikasi atau laporan yang setara secara substansial.

1.3 Supplier will: (a) upon request, promptly provide to Kyndryl a copy of each certification and report Supplier is obligated to obtain and (b) promptly resolve any internal control weaknesses noted during the SOC 2 or substantially equivalent (if Kyndryl so approves) reviews.

1.3 Pemasok akan: (a) atas permintaan, segera memberikan kepada Kyndryl salinan masing-masing sertifikasi dan laporan yang wajib didapatkan oleh Pemasok dan (b) segera menyelesaikan setiap kelemahan kontrol internal yang tercatat selama tinjauan SOC 2 atau tinjauan yang setara secara substansial (jika Kyndryl menyetujui).

Article X, Cooperation, Verification and Remediation

This Article applies if Supplier provides any Services or Deliverables to Kyndryl.

1. Supplier Cooperation

1.1 If Kyndryl has reason to question whether any Services or Deliverables may have contributed, are contributing or will contribute to any cyber security concern, then Supplier will reasonably cooperate with any Kyndryl inquiry regarding such concern, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Supplier Personnel, or the like.

1.2 The parties agree to: (a) furnish upon request to each other such further information, (b) execute and deliver to each other such other documents, and (c) do such other acts and things, all as the other party may reasonably request for the purpose of carrying out the intent of these Terms and the documents referred to in these Terms. For example, if Kyndryl requests, Supplier will timely provide the privacy and security focused terms of its written contracts with Subprocessors and subcontractors, including, where Supplier has the right to do so, by granting access to the contracts themselves.

1.3 If Kyndryl requests, Supplier will timely provide information on the countries where its Deliverables and the components of those Deliverables were manufactured, developed, or otherwise sourced.

2. Verification (as used below, "Facility" means a physical location where Supplier hosts, processes or otherwise accesses Kyndryl Materials)

2.1 Supplier will maintain an auditable record demonstrating compliance with these Terms.

Pasal X, Kerja Sama, Verifikasi dan Remediasi

Pasal ini berlaku jika Pemasok menyediakan setiap Layanan atau Materi yang Disampaikan kepada Kyndryl.

1. Kerja Sama Pemasok

1.1 Apabila Kyndryl memiliki alasan untuk mempertanyakan apakah setiap Layanan atau Materi yang Disampaikan mungkin telah berkontribusi, tengah berkontribusi, atau akan berkontribusi pada setiap persoalan keamanan siber, maka Pemasok akan bekerja sama secara wajar dengan setiap pertanyaan Kyndryl terkait dengan persoalan tersebut, termasuk dengan menanggapi permintaan atas informasi sepenuhnya dan tepat waktu, baik melalui dokumen, catatan lain, wawancara Personel Pemasok yang relevan, atau sejenisnya.

1.2 Para pihak setuju untuk: (a) menyediakan informasi lebih lanjut kepada satu sama lain berdasarkan permintaan, (b) menandatangani dan menyampaikan dokumen tersebut kepada satu sama lain, dan (c) melakukan hal dan tindakan serupa lainnya, semua sebagaimana pihak lain dapat meminta secara wajar untuk tujuan melaksanakan maksud Syarat-Syarat ini dan dokumen yang direferensikan dalam Syarat-Syarat ini. Misalnya, jika Kyndryl meminta, Pemasok akan memberikan syarat-syarat yang berfokus pada kerahasiaan dan keamanan secara tepat waktu dalam kontrak tertulisnya dengan Subprosesor dan subkontraktor, termasuk, jika Pemasok memiliki hak untuk melakukannya, dengan memberikan akses ke kontrak itu sendiri.

1.3 Jika Kyndryl meminta, Pemasok akan memberikan informasi secara tepat waktu mengenai negara-negara di mana Materi yang Disampaikan dan komponen Materi yang Disampaikan tersebut diproduksi, dikembangkan, atau bersumber.

2. Verifikasi (sebagaimana yang digunakan di bawah ini, "Fasilitas" berarti lokasi fisik di mana Pemasok menyelenggarakan, memproses, atau mengakses Materi Kyndryl)

2.1 Pemasok akan mengelola catatan yang dapat diaudit yang mendemonstrasikan kepatuhan dengan Syarat-Syarat ini.

2.2 Kyndryl, by itself or with an external auditor, may, upon 30 Days prior written notice to Supplier, verify Supplier's compliance with these Terms, including by accessing any Facility or Facilities for such purposes, though Kyndryl will not access any data center where Supplier Processes Kyndryl Data unless it has a good faith reason to believe that doing so would provide relevant information. Supplier will cooperate with Kyndryl's verification, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Supplier Personnel, or the like. Supplier may offer proof of adherence to an approved code of conduct or industry certification or otherwise provide information to demonstrate compliance with these Terms, for Kyndryl's consideration.

2.2 Kyndryl, sendiri maupun dengan auditor eksternal, dapat, pada 30 Hari sebelum pemberitahuan tertulis kepada Pemasok, memverifikasi kepatuhan Pemasok dengan Syarat-Syarat ini, termasuk dengan mengakses setiap Fasilitas untuk tujuan tersebut, meski Kyndryl tidak akan mengakses setiap pusat data di mana Pemasok Memproses Data Kyndryl kecuali apabila memiliki alasan iktikad baik untuk meyakini bahwa dengan melakukan hal tersebut akan memberikan informasi yang relevan. Pemasok akan bekerja sama dengan verifikasi Kyndryl, termasuk menanggapi permintaan sepenuhnya dan tepat waktu atas informasi, baik melalui dokumen, catatan lain, wawancara Personel Pemasok terkait, atau sejenisnya. Pemasok dapat menawarkan bukti kepatuhan terhadap kode etik yang disetujui atau sertifikasi industri atau memberikan informasi untuk mendemonstrasikan kepatuhan dengan Syarat-Syarat ini, untuk pertimbangan Kyndryl.

2.3 A verification will not occur more than once in any 12 month period, unless: (a) Kyndryl is validating Supplier's remediation of concerns resulting from a previous verification during the 12 month period or (b) a Security Breach has arisen and Kyndryl wishes to verify compliance with obligations relevant to the breach. In either case, Kyndryl will provide the same 30 Days prior written notice as specified in Section 2.2 above, but the urgency of addressing a Security Breach may necessitate Kyndryl conducting a verification on less than 30 Days prior written notice.

2.3 Verifikasi tidak akan berjalan lebih dari sekali dalam setiap periode 12 bulan, kecuali apabila: (a) Kyndryl memvalidasi perbaikan masalah Pemasok sebagai hasil dari verifikasi sebelumnya selama periode 12 bulan atau (b) Pelanggaran Keamanan telah timbul dan Kyndryl ingin memverifikasi kepatuhan dengan kewajiban yang berkaitan dengan pelanggaran. Dalam kasus-kasus tersebut, Kyndryl akan memberikan pemberitahuan tertulis yang sama 30 Hari sebelumnya sebagaimana yang ditetapkan dalam Bagian 2.2 di atas, tetapi urgensi dalam menangani Pelanggaran Keamanan mungkin memerlukan Kyndryl untuk melakukan verifikasi dengan pemberitahuan tertulis kurang dari 30 Hari sebelumnya.

2.4. A regulator or other Controller may exercise the same rights as Kyndryl in Sections 2.2 and 2.3, with the understanding that a regulator may exercise any additional rights it has under the law.

2.4. Pembuat peraturan atau Pengontrol lain dapat melaksanakan hak yang sama dengan Kyndryl dalam Bagian 2.2 dan 2.3, dengan pemahaman bahwa pembuat peraturan dapat melaksanakan setiap hak tambahan yang dimilikinya berdasarkan hukum.

2.5 If Kyndryl has a reasonable basis for concluding that Supplier is not compliant with any of these Terms (whether such basis arises from a verification under these Terms or otherwise), then Supplier will promptly remediate such non-compliance.

2.5 Jika Kyndryl memiliki landasan yang beralasan untuk menyimpulkan bahwa Pemasok tidak patuh dengan setiap Syarat-Syarat ini (baik landasan tersebut timbul dari verifikasi berdasarkan Syarat-Syarat ini atau hal lain), maka Pemasok akan segera menyelesaikan ketidakpatuhan tersebut.

3. Anti-Counterfeiting Program

3. Program Antipemalsuan

3.1 If Supplier's Deliverables include electronic components (e.g., hard disk drives, solid-state drives, memory, central processing units, logic devices or cables), Supplier will maintain and follow a documented counterfeit prevention program to, first and foremost, prevent Supplier from providing counterfeit components to Kyndryl and, secondarily, promptly detect and remediate any case where Supplier mistakenly provides counterfeit components to Kyndryl. Supplier will impose this same obligation to maintain and follow a documented counterfeit prevention program on all of its suppliers that provide electronic components that are included in Supplier's Deliverables to Kyndryl.

3.1 Jika Materi yang Disampaikan Pemasok mencakup komponen elektronik (misalnya, hard disk drive, solid-state drive, memori, unit pemrosesan sentral, perangkat logis atau kabel), Pemasok akan mempertahankan dan mengikuti program pencegahan pemalsuan terdokumentasi untuk, pertama dan terutama, mencegah Pemasok dalam memberikan komponen palsu kepada Kyndryl, kedua, segera mendeteksi dan memperbaiki setiap kasus di mana Pemasok salah memberikan komponen palsu kepada Kyndryl. Pemasok akan membebankan kewajiban yang sama untuk mempertahankan dan mengikuti program pencegahan pemalsuan terdokumentasi pada semua pemasoknya yang memberikan komponen elektronik yang tercakup dalam Materi yang Disampaikan Pemasok kepada Kyndryl.

4. Remediation

4.1 If Supplier fails to comply with any of its obligations under these Terms, and that failure causes a Security Breach, then Supplier will correct the failure in its performance and remediate the harmful effects of the Security Breach, with such performance and remediation at Kyndryl's reasonable direction and schedule. If, however, the Security Breach arises from Supplier's provision of a multi-tenant Hosted Service, and consequently impacts many Supplier customers, including Kyndryl, then Supplier will, given the nature of the Security Breach, timely and appropriately correct the failure in its performance and remediate the harmful effects of the Security Breach, while affording due consideration to any Kyndryl input on such corrections and remediation.

4.2 Kyndryl will have the right to participate in the remediation of any Security Breach referenced in Section 4.1, as it believes appropriate or necessary, and Supplier will be responsible for its costs and expenses in correcting its performance and for the remediation costs and expenses that the parties incur with respect to any such Security Breach.

4.3 By way of example, remediation costs and expenses associated with a Security Breach could include those for detecting and investigating a Security Breach, determining responsibilities under

4. Perbaikan

4.1 Apabila Pemasok gagal mematuhi setiap kewajibannya berdasarkan Syarat-Syarat ini, dan kegagalan tersebut menyebabkan Pelanggaran Keamanan, maka Pemasok akan mengoreksi kegagalan dalam kinerjanya dan melakukan perbaikan dampak berbahaya dari Pelanggaran Keamanan, dengan kinerja dan perbaikan tersebut atas arahan dan jadwal Kyndryl secara wajar. Namun, jika Pelanggaran Keamanan timbul dari pengadaan Layanan yang di-Host multipenyewa oleh Pemasok, dan akibatnya berdampak pada banyak pelanggan Pemasok, termasuk Kyndryl, maka Pemasok akan, berdasarkan sifat Pelanggaran Keamanan, mengoreksi kegagalan secara tepat waktu dan sesuai dalam kinerjanya dan melakukan perbaikan dampak yang berbahaya dari Pelanggaran Keamanan, sembari mengupayakan pertimbangan yang sepatutnya atas masukan Kyndryl pada koreksi dan perbaikan tersebut.

4.2 Kyndryl akan berhak untuk berpartisipasi dalam perbaikan setiap Pelanggaran Keamanan yang direferensikan dalam Bagian 4.1, sebagaimana diyakini tepat atau perlu, dan Pemasok akan bertanggung jawab atas biaya dan pengeluarannya dalam mengoreksi kinerjanya dan untuk biaya dan pengeluaran perbaikan yang dikeluarkan oleh para pihak sehubungan dengan Pelanggaran Keamanan tersebut.

4.3 Sebagai contoh, biaya dan pengeluaran perbaikan yang terkait dengan Pelanggaran Keamanan dapat mencakup biaya dan pengeluaran

applicable laws and regulations, providing breach notifications, establishing and maintaining call-centers, providing credit monitoring and credit restoration services, reloading data, correcting product defects (including through Source Code or other development), retaining third-parties to assist with the foregoing or other relevant activities, and other costs and expenses that are necessary to remediate the harmful effects of the Security Breach. For clarity, remediation costs and expenses would not include Kyndryl's loss of profits, business, value, revenue, goodwill, or anticipated savings.

untuk mendeteksi dan menyelidiki Pelanggaran Keamanan, menentukan tanggung jawab berdasarkan peraturan perundang-undangan dan regulasi yang berlaku, memberikan pemberitahuan pelanggaran, membangun dan mengelola pusat bantuan, memberikan layanan pemantauan kredit dan restorasi kredit, memuat ulang data, mengoreksi kerusakan produk (termasuk melalui Kode Sumber atau pengembangan lain), mempertahankan pihak ketiga untuk membantu aktivitas sebelumnya atau aktivitas relevan lainnya, serta biaya dan pengeluaran lain yang diperlukan untuk melakukan perbaikan dampak yang berbahaya dari Pelanggaran Keamanan. Untuk kejelasan, biaya dan pengeluaran untuk perbaikan tidak akan mencakup kehilangan laba, bisnis, nilai, pendapatan, nama baik, atau penghematan yang diharapkan Kyndryl.

This document is made in the English and Indonesian languages. To the extent permitted by the prevailing law, the English language of this document will prevail in the case of any inconsistencies or differences of interpretation with the Indonesian language text of this document.

Dokumen ini dibuat dalam bahasa Inggris dan bahasa Indonesia. Sepanjang diperbolehkan oleh hukum yang berlaku, dalam hal terdapat ketidaksesuaian atau perbedaan penafsiran dengan teks bahasa Indonesia dari dokumen ini, maka teks dalam bahasa Inggris yang akan berlaku.