제 I 조, 업무상 연락정보(BCI)

고객 또는 Kyndryl 이 상대방의 BCI 를 처리하는 경우 본 조항이 적용됩니다.

1.1 Kyndryl 및 공급자는 공급자의 서비스 및 인도물 제공과 관련하여 업무를 수행하는 어디서나 상대방의 BCI 를 처리할 수 있습니다.

1.2 당사자는 다음을 수행합니다.

a) 기타 다른 용도를 위해서는 상대방의 BCI 를 사용하거나 공개하지 않습니다(즉, 당사자는 상대방의 사전 서면 동의 없이, 그리고 필요한 경우 해당 데이터 주체의 사전 서면 동의 없이는 상대방의 BCI 를 판매하거나 상대방의 BCI 를 마케팅 목적으로 사용하거나 공개하지 않습니다). 및

b) 상대방의 서면 요청에 따라 즉시 상대방의 BCI 를 삭제, 수정, 정정, 반환하거나 상대방의 BCI 처리 관련 정보를 제공하거나 상대방의 BCI 처리를 제한하거나 상대방의 BCI 와 관련하여 합리적으로 요청된 기타 조치를 수행합니다.

1.3 당사자들은 서로의 BCI 와 관련한 공동 관리자 관계를 구성하지 않으며 거래서류의 어떠한 조항도 공동 관리자 관계를 설정하려는 의도를 나타내는 것으로 해석되거나 이해되지 않습니다.

1.4 https://www.kyndryl.com/privacy 의 Kyndryl 개인정보처리방침에는 Kyndryl 의 BCI 처리에 대한 추가 상세한 내용이 기재되어 있습니다.

1.5 당사자는 상대방의 BCI 를 유실, 파기, 변경, 우발적 또는 무단 공개, 우발적 또는 무단 액세스, 불법적 처리로부터 보호하기 위해 기술적 및 관리적 보안 조치들을 구현하였으며 앞으로 유지 관리할 것입니다.

1.6 공급자는 Kyndryl 의 BCI 와 관련된 보안 위반을 알게 된 후 즉시(그리고 어떤 경우에도 48 시간 이내에) Kyndryl 에 알립니다. 공급자는(이)라는 알림을 cyber.incidents@kyndryl.com 에 제공합니다. 공급자는 Kyndryl 에 그러한 위반 및 공급자의 시정 및 복원 활동 상태에 대한 합리적으로 요청된 정보를 제공합니다. 예를 들어, 합리적으로 요청된 정보에는 디바이스, 시스템 또는 애플리케이션, 관리 및 기타 액세스 권한, 디바이스, 시스템 또는 애플리케이션의 포렌식 이미지 및 기타 유사한 항목을 위반 사항이나 공급자의 시정 및 복원 활동과 관련한 범위 내에서 보여주는 보호된 로그가 포함될 수 있습니다.

1.7 공급자가 Kyndryl 의 BCI 를 처리만 하고 일체의 기타 다른 데이터나 자료 또는 Kyndryl 회사 시스템에 대한 액세스 권한이 없는 경우, 그러한 처리에는 본 조항 및 제 X 조 (협력, 확인 및 시정 조치)만 적용됩니다.

제 II 조, 기술적 및 관리적 조치들, 데이터 보안

공급자가 Kyndryl 의 BCI 외의 Kyndryl 데이터를 처리하는 경우 본 조항이 적용됩니다. 공급자는 모든 서비스 및 인도물을 제공하면서 본 조항의 요구사항을 준수하고 이로써 Kyndryl 데이터를 유실, 파기, 변경, 우발적 또는 무단 공개, 우발적 또는 무단 액세스 및 불법적 처리로부터 보호합니다. 본 조항의 요구사항은 모든 개발, 테스트, 호스팅, 지원, 운영 및 데이터 센터 환경을 비롯하여, 인도물 및 서비스를 제공하고 Kyndryl 기술을 핸들링하기 위해 공급자가 작동하거나 관리하는 모든 IT 애플리케이션, 플랫폼 및 인프라로 확대됩니다.

1. 데이터 사용

1.1. 공급자는 Kyndryl 의 사전 서면 동의 없이 개인 데이터를 포함하여 기타 다른 정보나 데이터를 Kyndryl 데이터에 추가하거나 포함시킬 수 없습니다. 또한 공급자는 서비스 및 인도물을 제공하는 것 이외의 목적으로 통합 또는 기타 어떠한 형태로도 Kyndryl 데이터를 사용할 수 없습니다(예: 공급자는 공급자의 오퍼링 개선 효과와 수단을 평가하거나 새로운 오퍼링을 생성하기 위한 연구 및 개발을 위해 또는 공급자의 오퍼링에 관한 보고서를 작성하기 위해 Kyndryl 데이터를 사용하거나 재사용할 수 없습니다). 거래서류에서 명시적으로 허용하지 않는 한, 공급자는 Kyndryl 데이터를 판매할 수 없습니다.

1.2. 공급자는 거래서류에서 명시적으로 허용하지 않는 한 웹 추적 기술을 인도물 내에 또는 서비스의 일부로 내장하지 않습니다(해당 기술에는 HTML5, 로컬 스토리지, 제 3 자 태그 또는 토큰 및 웹 비콘이 포함됨).

2. 제 3 자 요청사항들 및 기밀 보호

2.1. 공급자는 Kyndryl 이 사전에 서면으로 허가하지 않는 한, Kyndryl 데이터를 제 3 자에게 공개하지 않습니다. 규제 기관을 비롯한 정부가 Kyndryl 데이터에 대한 액세스를 요구하는 경우(예: 미국 정부가 Kyndryl 데이터를 얻기 위해 공급자에 국가 보안 명령을 이행하는 경우), 또는 달리 법령에서 Kyndryl 데이터의 공개를 요구하는 경우, 공급자는 그러한 요구나 요구사항을 Kyndryl 에게 서면으로 통지하고 공개에 대해 이의를 제기할 수 있는 합리적인 기회를 Kyndryl 에게 제공합니다(법령에서 통지를 금지하는 경우 공급자는 사법 조치나 기타 수단을 통해 금지 및 Kyndryl 데이터 공개에 이의를 제기하기 위해 적절하다고 합리적으로 판단되는 조치를 취합니다).

2.2. 공급자는 다음을 Kyndryl 에 보장합니다: (a) 서비스 또는 인도물을 제공하기 위해 Kyndryl 데이터의 액세스가 필요한 공급자 직원만 서비스 및 인도물을 제공하는 데 필요한 범위에 한해 액세스 권한을 가지며, (b) 해당 공급자 직원에게는 본 조항에서 허용하는 바에 따라서만 Kyndryl 데이터를 사용하고 공개하도록 하는 기밀 유지 의무를 적용합니다.

3. Kyndryl 데이터 반환 또는 삭제

3.1. 공급자는 거래서류의 종료 또는 만료 시에, 또는 Kyndryl 요청 시 사전에, Kyndryl 의 선택에 따라 Kyndryl 데이터를 삭제하거나 Kyndryl 에 반환합니다. Kyndryl 이 삭제를 요구하는 경우, 공급자는 업계 우수 사례에 따라, 데이터를 읽을 수 없고 재조립 또는 재구성할 수 없도록 하고 삭제 사실을 Kyndryl 에게 인증합니다. Kyndryl 이 Kyndryl 데이터의 반환을 요구하는 경우에는 공급자는 Kyndryl 의 합리적인 일정과 Kyndryl 의 합리적인 서면 지침에 따라 이를 수행합니다.

제 III 조, 개인정보 보호

공급자가 Kyndryl 개인 데이터를 처리하는 경우 본 조항이 적용됩니다.

1. 처리

1.1 Kyndryl 은 본 약관, 거래서류 및 당사자들 간의 연관 기본 계약의 지침을 비롯한 Kyndryl 의 지침에 따라 인도물과 서비스를 제공하기 위한 용도로만 Kyndryl 개인 데이터를 처리하는 처리자로 공급자를 지정합니다. 공급자가 지침을 수용하지 않는 경우 Kyndryl 은 서비스에서 영향을 받는 부분을 서면 통지로 해지할 수 있습니다. 공급자가 지침이 데이터 보호법을 위반한다고 판단되면 공급자는 이를 즉시 그리고 법령에서 요구하는 시간 범위 내에 Kyndryl 에 알립니다.

1.2 공급자는 서비스 및 인도물에 적용되는 모든 데이터 보호법을 준수합니다.

1.3 거래서류의 별표나 거래서류 자체에는 Kyndryl 데이터와 관련한 다음 사항이 명시됩니다.

(a) 데이터 주체의 카테고리,
(b) Kyndryl 개인 데이터의 유형,
(c) 데이터 조치 및 처리 활동;
(d) 처리 기간 및 빈도; 및
(e) 재처리자 목록.

2. 기술적 및 관리적 조치들(Technical and Organizational Measures, TOMs)

2.1 공급자는 제 II 조 (기술적 및 관리적 조치들, 데이터 보안) 및 제 VIII 조 (기술적 및 관리적 조치들, 일반 보안)에 명시된 기술적 및 관리적 조치들을 구현하고 유지 관리하며, 이를 통해 서비스 및 인도물에 존재하는 리스크에 대한 적절한 수준의 보안을 보장합니다. 공급자는 제 II 조, 본 III 조 및 제 VIII 조의 제한사항을 인증하고 이해하며 이를 준수합니다.

3. 데이터 주체의 권리 및 요청

3.1 공급자는 Kyndryl 개인 데이터와 관련하여 데이터 주체 권리(예: 데이터 수정, 삭제 또는 차단)를 행사하는 데이터 주체의 요청을 (Kyndryl 과 기타 관리자가 법적 의무를 이행할 수 있는 일정에 따라) Kyndryl 에게 즉시 통지합니다. 또한 공급자는 이러한 요청을 Kyndryl 에 하도록 데이터 주체에게 즉시 지시할 수 있습니다. 공급자는 Kyndryl 이 법적으로 요구하거나 서면으로 지시하지 않는 한 데이터 주체의 요청에 응답하지 않습니다.

3.2 Kyndryl 이 Kyndryl 개인 데이터와 관련된 정보를 기타 관리자나 기타 제 3 자(예: 데이터 주체 또는 규제 기관)에 제공해야 하는 경우, 공급자는 그러한 기타 관리자나 제 3 자에 대해 Kyndryl 이 적시에 대응할 수 있는 일정에 따라, Kyndryl 이 요청하는 정보를 제공하고 기타 합리적인 조치를 취함으로써 Kyndryl 을 지원합니다.

4. 재처리자(Subprocessors)

4.1 공급자는 재처리자를 새로 추가하거나 기존 재처리자의 처리 범위를 확대하기 전에 Kyndryl 에 사전에 서면으로 통지하며 사전 서면 통지에는 재처리자의 이름을 명시하고 신규 또는 확대되는 처리 범위에 대해 설명합니다. Kyndryl 은 새로운 재처리자 또는 처리 범위의 확대에 대해 합리적인 근거에 따라 언제든지 반대할 수 있으며 이 경우 당사자들은 Kyndryl 의 반대를 해결하기 위해 선의로 협력합니다. Kyndryl 이 언제든지 반대할 수 있는 그러한 권리에 따라

공급자의 서면 통지일로부터 30 일 이내에 달리 이의를 제기하지 않으면 공급자는 새로운 재처리자를 지명하거나 기존 재처리자의 처리 범위를 확대할 수 있습니다.

4.2 공급자는 재처리자가 여하한 Kyndryl 데이터를 처리하기 전에, 본 약관의 데이터 보호, 보안 및 인증 의무를 승인된 각 재처리자에게 부과합니다. 공급자는 각 재처리자의 의무 이행과 관련하여 Kyndryl 에 대해 전적으로 책임을 집니다.

5. 국외이전 데이터 처리

아래 용어는 다음과 같이 사용됩니다.

적합 국가(Adequate Country)는 해당 데이터 보호법이나 규제 기관의 의사결정에 따라 관련 전송에 관하여 적절한 수준의 데이터 보호를 제공하는 국가를 의미합니다.

데이터 Importer(Data Importer)는 적합 국가에 설립되지 않은 처리자 또는 재처리자를 의미합니다.

EU 표준 계약 조항(EU Standard Contractual Clauses)("EU SCCs")은 https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en 에 공식 게시된 대로, 조항 9(a)의 옵션 1 및 조항 17 의 옵션 2 를 제외하고 적용되는 선택적 조항이 포함된 EU 표준 계약 조항(EU Standard Contractual Clauses)(Commission Decision 2021/914)을 의미합니다.

세르비아 표준 계약 조항("Serbian SCC") 은 https://www.poverenik.rs/images/stories/dokumentacija-nova/podzakonski-akti/Klauzulelat.docx 에 게시된 "세르비아 공적 중요정보 및 개인 데이터 보호 위원정보에 대한 세르비아 위원"이 채택한 세르비아 표준 계약 조항을 의미합니다.

표준 계약 조항(Standard Contractual Clauses)("SCCs")은 적합 국가에 설립되지 않은 처리자에게 개인 데이터를 전송하는 경우에 관련 데이터 보호법에서 요구하는 계약 조항을 의미합니다.

EU Commission 표준 계약 조항에 대한 영국 국제 데이터 전송 부록("UK 부록")은 https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-Transfer-agreement-and-guidance/에 공식적으로 게시된 EU Commission 표준 계약 조항에 대한 영국 국제 데이터 전송 부록을 의미합니다.

5.1 공급자는 Kyndryl 의 사전 서면 동의 없이 Kyndryl 개인 데이터를 국외로 (원격 액세스 포함) 전송하거나 공개하지 않습니다. Kyndryl 이 동의하는 경우에는 당사자들은 관련 데이터 보호법을 준수하기 위해 협력합니다. 해당 법령에서 SCCs 를 요구하는 경우 공급자는 Kyndryl 의 요청에 따라 즉시 SCCs 를 체결합니다.

5.2 EU SCCs 와 관련하여 다음이 적용됩니다.

(a) 공급자가 적합 국가에 설립되지 않은 경우: 공급자는 데이터 Importer 로서 Kyndryl 과 EU SCCs 를 체결합니다. 그리고 공급자는 승인된 각 재처리자와 EU SCCs 의 9 절에 따라 서면 계약을 체결하고, 요청에 따라 계약서의 사본을 Kyndryl 에게 제공합니다.

(i) EU SCC 의 모듈 1 은 당사자가 서면으로 달리 합의하지 않는 한 적용되지 않습니다.

(ii) Kyndryl 이 관리자인 경우 EU SCC 의 모듈 2 가 적용되고 Kyndryl 이 처리자인 경우 모듈 3 이 적용됩니다. EU SCC 의 조항 13 에 따라 모듈 2 또는 3 이 적용될 때 당사자는 (1) EU SCC 가 관할 감독 기관이 위치한 EU 회원국의 법의 적용을 받고 (2) EU SCC 에서 발생하는 분쟁은 관할 감독 기관이 위치한 EU 회원국 법원에서 관할함을 동의합니다. (1)의 해당 법률이 제 3 자의 수혜권을 허용하지 않는 경우, EU SCC 는 네덜란드 법의 적용을 받으며 (2)에 따른 EU SCC 에서 발생하는 모든 분쟁은 네덜란드 암스테르담 법원의 결정에 따릅니다.

(b) 공급자가 유럽 경제 지역에 설립되고 Kyndryl 이 일반 데이터 보호 규정 2016/679 의 적용을 받지 않는 관리자인 경우, EU SCC 의 모듈 4 가 적용되며 공급자는 이에 따라 Kyndryl 과 데이터 exporter 로서 EU SCC 에 가입합니다. EU SCC 의 모듈 4 가 적용되는 경우 당사자는 EU SCC 에 네덜란드 법이 적용되며 EU SCC 에서 발생하는 모든 분쟁은 네덜란드 암스테르담 법원에서 해결하는 데 동의합니다.

(c) 고객 또는 계열사와 같은 기타 관리자가 7 항의 '도킹 조항'에 따라 EU SCC 의 당사자가 되기를 요청하는 경우 공급자는 이에 따라 이러한 요청에 동의합니다.

(d) EU SCC 의 부록 II 를 완료하는 데 필요한 기술적 및 관리적 조치는 본 약관, 거래서류 자체 및 당사자 간의 관련 기본 계약에서 찾을 수 있습니다.

(e) EU SCCs 와 본 약관이 상충하는 경우에는 EU SCCs 가 우선하여 적용됩니다.

5.3 UK SCCs 와 관련하여 다음이 적용됩니다.

(a) 공급자가 적합 국가에 설립되지 않은 경우: (i) 공급자는 공급자를 대신하여 데이터 Importer 로서 Kyndryl 과 UK SCCs 를 체결합니다. 그리고 (ii) 공급자는 데이터 Importer 인 승인된 각 재처리자와 UK SCCs 의 11 절에 따라 서면 계약을 체결하고, 요청에 따라 계약서의 사본을 Kyndryl 에게 제공합니다.

(b) 공급자가 적합 국가에 설립된 경우, 공급자는 데이터 Importer 인 각 재처리자를 대신하여 Kyndryl 과 UK SCCs 를 체결합니다. 공급자가 그러한 재처리자를 대신할 수 없는 경우, 공급자는 재처리자의 Kyndryl 개인 데이터 처리를 허용하기 전에 Kyndryl 의 서명에 대해 재처리자가 서명한 UK SCCs 를 Kyndryl 에 제공합니다.

(c) Kyndryl 과 공급자 간의 UK SCCs 는 사실 관계에 따라, 관리자와 처리자 간의 UK SCCs 로, 또는 UK SCCs 의 11 절에 따라 '데이터 Importer'와 '재처리자' 간의 back-to-back 서면 계약으로 사용됩니다. UK SCCs 와 본 약관이 상충하는 경우에는 UK SCCs 가 우선하여 적용됩니다.

(d) 고객, 계열사 등의 기타 관리자는 추가 '데이터 Exporters'가 되기를 요청할 수 있습니다. 공급자는 공급자를 대신하여 그리고 재처리자를 대신하여 그러한 요청에 동의하게 됩니다. Kyndryl 은 공급자에게 추가 '데이터 Exporters'에 대해 알리고 다시, 공급자는 데이터 Importers 인 재처리자에게 그러한 추가 '데이터 Exporters'에 대해 알립니다.

5.4 UK 부록과 관련하여 다음이 적용됩니다.

a) 공급자가 적합 국가에 설립되지 않은 경우: (i) 공급자가 위에 명시된 EU SCCs 에 추가하기 위해 Importer 로서 Kyndryl 과 UK 부록을 체결합니다(해당되는 경우, 처리 활동에 따라). 그리고 (ii) 공급자는 승인된 각 재처리자와 서면 계약을 체결합니다. 그리고 요청 시 Kyndryl 에게 계약서 사본을 제공합니다.

b) 공급자가 적합 국가에 설립되어 있고 Kyndryl 이 일반 데이터 보호 규정(2018 년 유럽연합 법에 따라 영국 법률에 통합됨)의 적용을 받지 않는 관리자인 경우, 공급자는 위의 5.2(b)절에 명시된 EU SCCs 에 추가하기 위해 Kyndryl 과 Exporter 로서 UK 부록을 체결합니다.

c) 고객 또는 계열사와 같은 기타 관리자가 UK 부록의 당사자가 되기를 요청하는 경우 공급자는 이에 따라 이러한 요청에 동의합니다.

d) UK 부록의 부록 정보(표 3 에 명시된 바와 같이)는 해당 EU SCCs, 본 약관, 거래 문서 자체 및 당사자 간의 관련 기본 계약에서 확인할 수 있습니다. Kyndryl 또는 공급자는 UK 부록이 변경될 때 UK 부록을 종료할 수 없습니다.

e) UK 부록과 본 약관이 상충하는 경우에는 UK 부록이 우선하여 적용됩니다.

5.5 Serbian SCCs 와 관련하여 다음이 적용됩니다.

(a) 공급자가 적합 국가에 설립되지 않은 경우: (i) 공급자는 처리자로서 공급자를 대신하여 Kyndryl 과 Serbian SCC 를 체결합니다. 그리고 (ii) 공급자는 Serbian SCC 제 8 조에 따라 승인된 각 재처리자와 서면 계약을 체결하고 요청 시 해당 계약의 사본을 Kyndryl 에 제공합니다.

(b) 공급자가 적합 국가에 설립된 경우 공급자는 부적합 국가에 있는 각 재처리자를 대신하여 Kyndryl 과 Serbian SCC 를 체결합니다. 공급자가 그러한 재처리자를 대신할 수 없는 경우, 공급자는 재처리자의 Kyndryl 개인 데이터 처리를 허용하기 전에 Kyndryl 의 서명에 대해 재처리자가 서명한 Serbian SCCs 를 Kyndryl 에 제공합니다.

(c) Kyndryl 과 공급자 간의 Serbian SCCs 는 사실 관계에 따라, 관리자와 처리자 간의 Serbian SCCs 로, 또는 '처리자'와 '재처리자' 간의 back-to-back 서면 계약으로 사용됩니다. Serbian SCCs 와 본 약관이 상충하는 경우에는 Serbian SCCs 가 우선하여 적용됩니다.

(d) 부적합 국가에 대한 개인 데이터의 전송을 규정하기 위한 세르비아 SCC 부록 1 – 8 을 완료하는 데 필요한 정보는 본 약관과 거래서류의 별표 또는 거래서류 자체에서 찾을 수 있습니다.

6. 지원 및 기록

6.1 처리의 성격을 고려하여, 공급자는 데이터 주체의 요청 및 권리와 관련한 의무 이행을 위해 적절한 기술적 및 관리적 조치들을 보유함으로써 Kyndryl 을 지원합니다. 또한 공급자는 공급자가 이용할 수 있는 정보를 고려하여 필요한 경우, 담당 규제 기관과 사전 협의하는

것을 포함하여, 처리 보안, 보안 위반 통지 및 의사교환, 데이터 보호 영향 평가서 작성과 관련된 의무를 준수할 수 있도록 Kyndryl 을 지원합니다.

6.2 공급자는 각 재처리자의 대표 및 데이터 보호 담당자를 포함하여, 각 재처리자의 이름과 연락처 세부사항에 대한 최신 기록을 유지합니다. 요청에 따라, 공급자는 이 기록을 Kyndryl 이 고객이나 기타 제 3 자의 요구에 적시에 응대할 수 있는 일정에 맞추어 Kyndryl 에게 제공합니다.

제 IV 조, 기술적 및 관리적 조치들, 코드 보안

공급자가 Kyndryl 소스 코드에 대한 액세스 권한이 있는 경우 본 조항이 적용됩니다. 공급자는 본 조항의 요구사항을 준수하며 이로써 Kyndryl 소스 코드를 유실, 파기, 변경, 우발적 또는 무단 공개, 우발적 또는 무단 액세스 및 불법적 핸들링으로부터 보호합니다. 본 조항의 요구사항은 모든 개발, 테스트, 호스팅, 지원, 운영 및 데이터 센터 환경을 포함하여, 공급자가 인도물과 서비스를 제공하고 Kyndryl 기술을 핸들링하기 위해 작동하거나 관리하는 모든 IT 애플리케이션, 플랫폼 및 인프라로 확대됩니다.

1. 보안 요구사항

아래 용어는 다음과 같이 사용됩니다.

금지 국가(Prohibited Country)란 (a) 미국 정부가 2019 년 5 월 15 일 정보 통신 기술 및 서비스 공급망 보안에 관한 행정 명령(Executive Order on Securing the Information and Communications Technology and Services Supply Chain)에 따라 적국으로 지정하였거나 (b) 2019 년 미국 국방 수권법(the U.S. National Defense Authorization Act of 2019) 제 1654 조에 따라 명시되었거나, 또는 (c) 거래서류에서 "금지 국가"로 명시된 여하한 국가를 의미합니다.

1.1. 공급자는 Kyndryl 소스 코드를 제 3 자의 이익을 위해 배포하거나 임치(escrow)하지 않습니다.

1.2. 공급자는 Kyndryl 소스 코드가 금지 국가에 소재한 서버에 배치되도록 허용하지 않습니다. 공급자는 금지 국가에 소재하거나 금지 국가를 방문하는 공급자 직원을 포함한 개인은 (그러한 방문의 범위 내에서), Kyndryl 소스 코드가 전세계에 위치한 장소에 상관 없이 어떠한 이유로든 Kyndryl 소스 코드에 액세스하거나 사용하는 것을 허용하지 않으며, 그러한 액세스나 사용을 필요로 하는 개발, 테스트 또는 기타 작업이 금지 국가에서 수행되는 것을 허용하지 않습니다.

1.3. 공급자는 법령 또는 법령의 해석을 위해 제 3 자에 대한 Kyndryl 소스 코드의 공개가 요구되는 국가에는 Kyndryl 소스 코드를 배치하거나 배포하지 않습니다. Kyndryl 소스 코드가 배치된 국가에서 법령이나 법령의 해석에 대한 변경사항이 발생하여 해당 소스 코드를 제 3 자에게 공개해야 하는 경우, 공급자는 Kyndryl 소스 코드를 해당 국가에서 즉시 파기하거나 삭제하고 해당 법령이나 법령의 해석이 여전히 유효하면 해당 국가에서 Kyndryl 소스 코드를 추가로 배치하지 않습니다.

1.4. 공급자는 공급자, Kyndryl 또는 제 3 자로하여금 2019 년 미국 국방 수권법(the U.S. National Defense Authorization Act of 2019) 제 1654 조 또는 제 1655 조에 의거 공개 의무를 발생시킬 수 있는 어떠한 조치(계약의 체결 포함)도 직접 또는 간접적으로 취하지 않습니다. 즉, 거래서류 또는 당사자들 간의 관련 기본 계약에 따라 명시적으로 허용될 수 있는 경우를 제외하고, 공급자는 어떠한 경우에도 Kyndryl 의 사전 서면 동의 없이는 Kyndryl 소스 코드를 제 3 자에게 공개할 수 없습니다.

1.5. (a) 공급자가 금지 국가나 상기 1.3 항의 국가로 Kyndryl 소스 코드의 반입을 허용하였거나 (b) 공급자가 Kyndryl 소스 코드를 거래서류, 당사자들 간의 관련 기본 계약 또는 기타 계약에서 허용하지 않은 방식으로 달리 제공, 액세스 또는 사용하였거나 (c) 공급자가 상기 1.4 항을 위반하였다고 Kyndryl 이 공급자에게, 또는 제 3 자가 일방 당사자에게 통지한 경우, 법률이나 지분 또는 거래서류나 당사자들 간의 관련 기본 계약 또는 기타 계약에 따라 그러한 비준수를 해결하는 Kyndryl 의 권리를 제한하지 않고, (i) 그러한 통지가 공급자에게 제공된 경우 공급자는 통지사항을 즉시 Kyndryl 과 공유하고 (ii) Kyndryl 의 합리적인 지시와 Kyndryl 이 (공급자와 논의한 후) 합리적으로 결정한 일정에 따라 사안을 조사하고 해결합니다.

1.6. Kyndryl 은 공급자의 소스 코드 관련 정책, 절차, 관리 또는 관행에 대한 변경이 사이버 보안, 지적 재산권 도용 또는 유사하거나 관련성 있는 위험(그러한 변경 없이는 특정 고객이나 특정 시장에 대한 Kyndryl 의 판매가 제한되거나 고객의 보안 또는 공급망 요건이 충족되지

못하도록 할 수 있는 위험 포함)을 해소하는 데 필요하다고 합리적으로 판단되는 경우 공급자와 연락하여 그러한 정책, 절차, 관리 또는 관행의 변경을 포함하여, 위험을 해결하기 위해 필요한 조치를 논의할 수 있습니다. Kyndryl 의 요청에 따라, 공급자는 변경이 필요한지 평가하고 상호 합의된 적절한 변경을 구현하기 위해 Kyndryl 과 협력합니다.

제 V 조, 보안 개발

본 조항은 공급자가 자신 또는 제3자 소스 코드 또는 온프레미스 소프트웨어를 Kyndryl에게 제공하거나, 공급자의 인도물 또는 서비스가 Kyndryl 제품 또는 서비스의 일부로 Kyndryl 고객에게 제공되는 경우에 적용됩니다.

1. 보안 준비성

공급자는 공급자의 인도물을 기반으로 하는 Kyndryl 제품 및 서비스의 보안 준비성(정보 요청에 대해 적시에 완전하게 응대하는 방식 포함)을 문서, 기타 레코드, 관련 공급자 직원의 인터뷰 또는 기타 방법으로 평가하는 Kyndryl 의 내부 절차에 협력합니다.

2. 보안 개발

2.1 제 2 절은 공급자가 Kyndryl 에 온프레미스 소프트웨어를 제공하는 경우에만 적용됩니다.

2.2 공급자는 업계 모범 사례에 따라 거래서류 기간 동안 다음을 위해 필요한 네트워크, 플랫폼, 시스템, 애플리케이션, 디바이스, 물리적 인프라, 사고 대응 및 직원중심의 보안 정책, 절차 및 통제를 구현했으며 유지합니다. (a) 공급자 또는 공급자가 고용한 제 3 자가 인도물을 위해 또는 인도물과 관련하여 운영, 관리, 사용 또는 의존하는 개발, 구축, 테스트 및 운영 시스템 및 환경의 보호 및 (b) 손실, 불법적인 형태의 취급, 무단 액세스, 공개 또는 변경으로부터 모든 인도 가능 소스 코드의 보호.

3. ISO 20243 인증

3.1 제 3 절은 공급자의 인도물 또는 서비스가 Kyndryl 제품 또는 서비스의 일부로 Kyndryl 고객에게 제공되는 경우에만 적용됩니다.

3.2 공급자는 ISO 20243, 정보 기술, Open Trusted Technology Provider, TM Standard (O-TTPS), 악의적으로 오염 및 위조된 제품의 최소화 준수에 대한 인증(자체 평가 인증 또는 신뢰할 수 있는 독립적인 감사자의 평가에 기반한 인증 중 하나)을 확보합니다. 대안으로, 공급자가 서면으로 요청하고 Kyndryl 이 서면으로 승인하는 경우 공급자는 안전한 개발 및 공급망 관행을 다루는 실질적으로 동등한 산업 표준 준수에 대한 인증(Kyndryl 이 승인하는 경우 이에 따라, 자체 평가 인증 또는 신뢰할 수 있는 독립적인 감사자의 평가에 기반한 인증 중 하나)을 확보합니다.

3.3 공급자는 거래서류의 발효일 이후 180 일까지 ISO 20243 또는 (Kyndryl 이 서면으로 승인하는 경우) 실질적으로 동등한 산업 표준 준수 인증을 확보하고 이후 12 개월마다 인증을 갱신합니다(각각 최신 버전의 관련 표준 즉, ISO 20243 또는 Kyndryl 이 서면으로 승인한 경우 안전한 개발 및 공급망 관행을 다루는 실질적으로 동등한 산업 표준에 대해 갱신).

3.4 공급자는 요청에 따라, 상기 2.1 및 2.2 항에 준하여 공급자가 확보해야 하는 인증서의 사본을 Kyndryl 에게 즉시 제공합니다.

4. 보안 취약성

아래 용어는 다음과 같이 사용됩니다.

오류 수정은 인도물의 보안 취약성을 포함하여 오류 또는 결함을 수정하는 버그 수정 및 개정을 의미합니다.

완화는 보안 취약성의 위험을 줄이거나 피하는 알려진 수단을 의미합니다.

보안 취약성은 인도물의 설계, 코딩, 개발, 구현, 테스트, 운영, 지원, 유지 관리 또는 관리에서 무단 액세스 또는 악용을 초래할 수 있는 공격이 가능한 상태를 의미하며, 다음을 포함합니다 (a) 시스템에 대한 액세스, 시스템 운영에 대한 통제 또는 방해, (b) 데이터에 대한 액세스, 삭제, 변경 또는 추출 또는 (c) 사용자 또는 관리자의 신원, 허가 또는 권한 변경. CVE(Common Vulnerabilities and Exposures) ID 나 점수 또는 공식 분류가 지정되었는지 여부에 관계없이 보안 취약성이 존재할 수 있습니다.

4.1 공급자는 다음 사항을 진술하고 보증합니다. (a) 업계 우수 사례를 사용하여 지속적인 정적 및 동적 소스 코드 애플리케이션 보안 검색, 오픈 소스 보안 검색 및 시스템 취약성 검색을 통해 보안 취약성을 식별합니다. (b) 본 약관의 요구사항을 준수하여 인도물 및 공급자가 서비스 및 인도물을 작성하고 제공하는 모든 IT 애플리케이션, 플랫폼, 인프라의 보안 취약성을 예방, 탐지 및 수정하도록 돕습니다.

4.2 공급자가 인도물 또는 그러한 IT 애플리케이션, 플랫폼 또는 인프라의 보안 취약성을 알게 되면 공급자는 Kyndryl에 아래 표에 정의된 심각도 레벨 및 기간에 따라 인도물의 모든 버전 및 릴리스에 대한 오류 수정 및 완화를 제공합니다.

심각도 레벨*
긴급 보안 취약성 – 심각하여 잠재적으로 글로벌 위협이 되는 보안 취약성입니다. Kyndryl은 CVSS 기본 점수와 상관 없이 단독 재량으로 긴급 보안 취약성을 지정합니다.
심각 – CVSS 기본 점수가 9 ~ 10.0 인 보안 취약성입니다.
높음 – CVSS 기본 점수가 7.0 ~ 8.9인 보안 취약성입니다.
중간 – CVSS 기본 점수가 4.0 ~ 6.9 인 보안 취약성입니다.
낮음 – CVSS 기본 점수가 0.0 ~ 3.9 인 보안 취약성입니다.

기간				
긴급	***심각***	***높음***	***중간***	***낮음***
Kyndryl Chief Information Security Office 에서 결정한 바에 따라, 4 일 이하	30 일	30 일	90 일	업계 우수 사례별

* 보안 취약성에 CVSS 기본 점수가 쉽게 할당되지 않은 경우 공급자는 이러한 취약성의 특성 및 상황에 적합한 심각도 레벨을 적용합니다.

4.3 공급자는 아직 Kyndryl에 오류 수정 또는 완화를 제공하지 않은 대중에 공개된 보안 취약성에 대해 공급자는 기술적으로 실현 가능한 추가 보안 제어를 구현하여 취약성의 위험을 완화할 수 있습니다.

4.4 Kyndryl이 위에서 언급한 인도물 또는 애플리케이션, 플랫폼 또는 인프라의 보안 취약성에 대한 공급자의 대응에 불만이 있는 경우, Kyndryl의 어떤 권리에도 영향을 미치지 않고, 공급자는 Kyndryl이 오류 수정을 담당하는 공급자 부사장 또는 이와 동등한 임원과 직접 논의할 수 있도록 즉시 준비합니다.

4.5 보안 취약성의 예에는 더 이상 보안 수정사항이 제공되지 않는 제3자 코드 또는 EOS(End-of-Service) 오픈 소스 코드가 있습니다.

제 VI 조, 회사 시스템 액세스

공급자 직원이 회사 시스템에 대한 액세스 권한이 있는 경우 본 조항이 적용됩니다.

1. 일반 조건

1.1 Kyndryl 은 공급자 직원에게 회사 시스템에 대한 액세스 권한을 부여할 것인지 여부를 결정합니다. Kyndryl 이 권한을 부여하는 경우 공급자는 본 조항의 요구사항을 준수해야 하며 해당 액세스 권한이 있는 공급자 직원도 이를 준수하도록 해야 합니다.

1.2 Kyndryl 은 공급자 직원이 회사 시스템에 액세스하는 데 Kyndryl 이 제공한 디바이스를 사용할 것인지 또는 공급자가 제공한 디바이스를 사용할 것인지 여부를 포함하여, 공급자 직원이 회사 시스템에 액세스할 수 있는 방법을 명시합니다.

1.3 공급자 직원은 서비스를 제공하기 위해서만 회사 시스템에 액세스할 수 있고 해당 액세스 목적으로 Kyndryl 이 허용한 디바이스를 사용할 수 있습니다. 공급자 직원은 다른 개인이나 법인에게 서비스를 제공하거나, 서비스와 관련하여 공급자 또는 제 3 자의 IT 시스템, 네트워크, 애플리케이션, 웹 사이트, 이메일 도구, 협업 도구 등에 액세스하는 데는 Kyndryl 이 허용한 디바이스를 사용할 수 없습니다.

1.4 즉, 공급자 직원은 개인적 사유로는 회사 시스템에 액세스하도록 Kyndryl 이 허용한 디바이스를 사용할 수 없습니다(예를 들어, 음악, 비디오, 사진 또는 기타 유사한 항목과 같은 개인 파일을 해당 디바이스에 저장할 수 없으며 개인적인 사유로는 해당 디바이스에서 인터넷을 사용할 수 없습니다).

1.5 공급자 직원은 회사 시스템을 통해 액세스 가능한 Kyndryl 자료를 Kyndryl 의 사전 서면 승인 없이 복사하지 않(으며 USB, 외장 하드 드라이브 또는 기타 유사한 항목과 같은 휴대용 저장 장치에 Kyndryl 자료를 복사하지 않)습니다.

1.6 요청에 따라, 공급자는 Kyndryl 이 명시한 기간 동안 공급자 직원이 액세스 권한을 부여받고 액세스한 특정 회사 시스템을 직원 이름으로 확인합니다.

1.7 공급자는 회사 시스템 액세스 권한이 있는 공급자 직원이 더 이상 (a) 공급자에게 고용되지 않거나 (b) 액세스 권한이 필요한 활동을 수행하지 않는 경우 24 시간 이내에 이를 Kyndryl 에게 통지합니다. 공급자는 Kyndryl 과 협력하여 그러한 이전 직원이나 현재 직원의 액세스 권한을 즉시 취소하도록 합니다.

1.8 공급자는 실제 또는 의심되는 보안 사고(Kyndryl 또는 공급자 디바이스의 분실, 디바이스, 데이터, 자료 또는 기타 일체의 정보에 대한 무단 액세스 등)를 Kyndryl 에게 즉시 보고하고 사고 조사를 위해 Kyndryl 과 협력합니다.

1.9 공급자는 Kyndryl 의 사전 서면 동의 없이는 여하한 회사 시스템에 대한 대리인, 독립적인 계약자 또는 하도급자 직원의 액세스를 허용할 수 없습니다. Kyndryl 이 동의하는 경우 공급자는 해당 개인 및 개인의 고용주가 공급자의 직원인 것처럼 본 조항의 요구사항을 준수하도록 계약상으로 확약하고 회사 시스템 액세스와 관련하여 해당 개인 또는 고용주의 모든 행위 및 부작위에 대해 Kyndryl 에게 책임을 집니다.

2. 디바이스 소프트웨어

2.1 공급자는 회사 시스템에 안전하게 액세스하는 데 용이하도록 Kyndryl 이 요구하는 모든 디바이스 소프트웨어를 적시에 설치하도록 공급자 직원에게 지시합니다. 공급자 및 공급자 직원은 해당 소프트웨어 또는 해당 소프트웨어에서 사용되는 보안 기능의 작동을 방해하지 않습니다.

2.2 공급자 및 공급자 직원은 Kyndryl 이 정한 디바이스 구성 규칙을 준수하며 Kyndryl 이 의도한 대로 소프트웨어가 작동하도록 돕기 위해 Kyndryl 과 협력합니다. 예를 들어, 공급자는 소프트웨어 웹 사이트 차단 또는 자동 패치 기능을 중단시키지 않습니다.

2.3 공급자는 회사 시스템 액세스에 사용하는 디바이스, 디바이스 사용자 이름 또는 비밀번호 등을 다른 사람과 공유할 수 없습니다.

2.4 Kyndryl 이 공급자 직원에게 공급자 디바이스를 사용하여 회사 시스템에 액세스할 수 있도록 허용한 경우, 공급자는 Kyndryl 이 승인한 디바이스에 운영 체제를 설치하고 실행하며 Kyndryl 이 지시한 후 합리적인 시간 내에 운영 체제의 새 버전 또는 새 운영 체제로 업그레이드합니다.

3. 감독 및 협력

3.1 Kyndryl 은 공급자, 공급자 직원 또는 기타 사용자에 대한 별도의 사전 통지 없이 잠재적 침입 및 기타 사이버 보안 위협에 대해, 방식이나 장소의 구애 없이 필요하거나 적절하다고 판단되는 모든 수단을 동원하여 감시하고 개선할 수 있는 전적인 권리를 가집니다. 이러한 권리의 예로써, Kyndryl 은 언제든지, (a) 디바이스 보안 테스트를 수행하고 (b) 디바이스에 저장되거나 회사 시스템을 통해 전송된 통신문(이메일 계정의 이메일 포함), 레코드, 파일 및 기타 항목을 감시하고 기술적 또는 기타 방법으로 복구하고 검토하며 (c) 디바이스의 전체 포렌식 이미지를 확보할 수 있습니다. Kyndryl 이 권리를 행사하는 데 공급자의 협력이 필요한 경우, 공급자는 Kyndryl 의 협력 요청(예를 들어, 안전한 디바이스 구성, 디바이스에서 모니터링 또는 기타 소프트웨어 설치, 시스템 레벨 연결 세부사항 공유, 디바이스 사고 대응 조치의 참여, Kyndryl 의 전체 포렌식 이미지 확보를 위한 디바이스에 대한 물리적 액세스 제공에 대한 요청, 유사한 요청 및 관련성 있는 요청 포함)에 대해 완전하게 적시에 충족합니다.

3.2 Kyndryl은 Kyndryl을 보호하는 데 필요하다고 판단되는 경우 공급자 또는 공급자 직원에 대한 사전 통지 없이, 일부 공급자 직원 또는 모든 공급자 직원의 회사 시스템 액세스 권한을 언제든지 취소할 수 있습니다.

3.3 Kyndryl의 권리는, 모든 데이터, 자료 또는 기타 일체의 정보는 선별된 사업장에만 존재할 수 있도록 하는 조항이나 선별된 사업장의 사용자만 그러한 데이터, 자료 또는 기타 정보에 액세스할 수 있도록 하는 조항을 포함하여, 거래서류, 당사자들 간의 관련 기본 계약 또는 기타 계약의 어떠한 조항에 의해서도 어떤 방식으로든 저지되거나 축소되거나 제한되지 않습니다.

4. Kyndryl 디바이스

4.1 모든 Kyndryl 디바이스에 대한 소유권은 Kyndryl이 보유하며, 공급자는 도난, 기물 파손 또는 과실로 인한 경우를 포함하여, 디바이스에 대한 분실 위험을 감수합니다. 공급자는 Kyndryl의 사전 서면 동의 없이 디바이스 소프트웨어, 애플리케이션, 보안 설계, 보안 구성, 물리적, 기계적 또는 전기적 설계의 변경을 포함하여, 디바이스를 변화시키는 어떠한 Kyndryl 디바이스에 대한 개조도 수행하거나 허용하지 않습니다.

4.2 공급자는 서비스를 제공하기 위한 디바이스의 필요가 없어진 후 5 영업일 이내에 모든 Kyndryl 디바이스를 반환하며 Kyndryl이 요청하는 경우, 그러한 모든 데이터, 자료 및 기타 정보를 영구적으로 삭제하는 업계 우수 사례를 따라서 어떠한 사본도 보관하지 않고 해당 디바이스에 대한 모든 데이터, 자료 및 기타 일체의 정보를 동시에 파기합니다. 공급자는 자체 비용을 부담하여, Kyndryl 디바이스가 공급자에게 인도되었던 때와 동일한 상태(합리적인 마모는 제외)로 패킹하여 Kyndryl이 지정한 장소로 반환합니다. 어떤 계약에 따른 공급자의 작업이나 기타 활동이 회사 시스템에 대한 액세스로 인해 용이해진 경우 해당 계약은 "관련성이 있다"는

이해하에, 본 4.2 항의 의무에 대한 공급자의 미이행은 거래서류, 당사자들 간의 관련 기본 계약 및 관련성이 있는 계약에 대한 중대한 위반으로 간주됩니다.

4.3 Kyndryl은 Kyndryl 디바이스에 대해 지원(디바이스 검사, 예방 및 정비 보수 포함)을 제공합니다. 공급자는 정비 서비스가 필요한 경우 Kyndryl에게 즉시 알립니다.

4.4 Kyndryl은 Kyndryl이 소유하거나 라이센싱할 수 있는 소프트웨어 프로그램에 대해 Kyndryl 디바이스의 허가된 사용을 지원하기에 충분한 사본을 사용하고 저장하고 작성할 수 있는 임시 권리를 공급자에게 부여합니다. 공급자는 계약에 따른 권리포기 가능성 없이 관련 법령에서 구체적으로 허용하지 않는 한, 타인에게 프로그램을 양도하거나 소프트웨어 라이센스 정보의 사본을 작성하거나 프로그램을 해체, 디컴파일, 리버스 엔지니어 또는 달리 변환할 수 없습니다.

5. 업데이트

5.1 거래서류 또는 당사자들 간의 관련 기본 계약의 상반되는 어떠한 내용에도 불구하고, Kyndryl은 관련 법령이나 고객의 의무에 따른 요구사항을 해결하거나 보안 우수 사례의 개선점을 반영하거나 회사 시스템 또는 Kyndryl을 보호하는 데 필요하다고 판단되는 바에 따라 공급자에 대한 서면 통지로, 공급자의 동의 없이 본 조항을 업데이트, 보완 또는 달리 수정할 수 있습니다.

제 VII 조, 스탭 증대

공급자 직원이 모든 업무 시간을 Kyndryl 에 서비스를 제공하는 데 사용하고 Kyndryl 또는 고객의 근무 장소, 또는 가정에서 그러한 모든 서비스를 수행하며 Kyndryl 디바이스를 사용하여 회사 시스템에 액세스해서만 서비스를 제공하는 경우에 본 조항이 적용됩니다.

1. 회사 시스템 액세스, Kyndryl 환경

1.1 공급자는 Kyndryl이 제공하는 디바이스를 사용하여 회사 시스템에 액세스해서만 서비스를 수행할 수 있습니다.

1.2 공급자는 회사 시스템에 대한 모든 액세스에 대하여 제 VI 조 (회사 시스템 액세스)에 명시된 조건을 준수합니다.

1.3 Kyndryl이 제공한 디바이스는 공급자 및 공급자 직원이 서비스를 제공하는 데 사용할 수 있는 유일한 디바이스이며 서비스 제공을 위해서만 공급자 및 공급자 직원에 의해 사용될 수 있습니다. 즉, 어떠한 경우에도 공급자 또는 공급자 직원은 서비스를 제공하는 데 다른 디바이스를 사용하거나 Kyndryl 디바이스를 다른 공급자 고객을 위해 사용하거나 Kyndryl에게 서비스를 제공하기 위한 용도 외에는 사용할 수 없습니다.

1.4 Kyndryl 디바이스를 사용하는 공급자 직원은 Kyndryl 자료를 상호 공유하고 해당 자료를 Kyndryl 디바이스에 저장할 수 있지만 이는 그러한 공유와 저장이 성공적으로 서비스를 수행하는 데 필요한 경우로 한정됩니다.

1.5 그러한 Kyndryl 디바이스 내의 저장은 제외하고, 어떠한 경우에도 공급자 또는 공급자 직원은 Kyndryl 자료를 Kyndryl이 보유한 Kyndryl 저장소, 환경, 도구 또는 인프라에서 제거할 수 없습니다.

1.6 즉, 공급자 및 공급자 직원은 Kyndryl의 사전 서면 동의 없이 Kyndryl 자료를 공급자의 저장소, 환경, 도구, 인프라 또는 기타 공급자의 시스템, 플랫폼, 네트워크 등으로 전송할 수 없습니다.

1.7 공급자 직원이 Kyndryl에 대한 서비스를 제공하는 데 모든 업무 시간을 할애하고 그러한 모든 서비스를 Kyndryl 또는 고객의 근무 장소, 또는 가정에서 수행하며 Kyndryl 디바이스를 사용하여 회사 시스템에 액세스해서만 서비스를 제공하는 경우 제 VIII 조 (기술적 및 관리적 조치들, 일반 보안)은 공급자의 서비스에 적용되지 않습니다. 그렇지 않은 경우에는 제 VIII 조가 공급자의 서비스에 적용됩니다.

제 VIII 조, 기술적 및 관리적 조치들, 일반 보안

이 조항은 공급자가 Kyndryl 에 서비스 또는 산출물을 제공하거나(단, 공급자가 해당 서비스 및 인도물을 제공할 때 Kyndryl BCI 에만 액세스할 수 있는 경우는 예외로 함. 즉, 공급자는 다른 Kyndryl 데이터를 처리하거나 다른 Kyndryl 자료 또는 기업 시스템에 액세스할 수 없음), 공급자의 유일한 서비스 및 인도물은 온프레미스 소프트웨어를 Kyndryl 에 제공하는 것이거나 공급자가 제 1.7 절을 포함하여 제 VII 조에 따라 직원 보강 모델로 모든 서비스 및 인도물을 제공하는 경우에 적용됩니다.

공급자는 본 조항의 요구사항을 준수하며 이를 통해 (a) Kyndryl 자료를 유실, 파기, 변경, 우발적 또는 무단 공개 및 우발적 또는 무단 액세스로부터, (b) Kyndryl 데이터를 불법적 처리로부터 및 (c) Kyndryl 기술을 불법적 핸들링으로부터 보호합니다. 본 조항의 요구사항은 모든 개발, 테스트, 호스팅, 지원, 운영 및 데이터 센터 환경을 포함하여, 공급자가 인도물과 서비스를 제공하고 Kyndryl 기술을 핸들링하기 위해 작동하거나 관리하는 모든 IT 애플리케이션, 플랫폼 및 인프라로 확대됩니다.

1. 보안 정책

1.1. 공급자는 공급자의 비즈니스에 필수적이고 모든 공급자 직원에게 의무사항이며 업계 우수 사례에 부합하는 IT 보안 정책 및 실무를 유지 관리하고 준수합니다.

1.2. 공급자는 IT 보안 정책 및 실무를 최소한 매년 검토하고 Kyndryl 자료를 보호하기 위해 필요하다고 판단하는 바에 따라 수정합니다.

1.3. 공급자는 모든 신입 사원 고용에 대한 표준 필수 고용 검증 요구사항을 유지하고 준수하며 이러한 요구사항을 모든 공급자 직원 및 공급자의 완전소유 자회사로 확대합니다. 이러한 요구사항에는 현지법에서 허용하는 범위 내에서 범죄 이력 확인, 신원 확인 증명 및 공급자가 필요하다고 판단되는 추가 검사가 포함됩니다. 공급자는 필요에 따라 이러한 요구사항을 정기적으로 반복하고 재확인합니다.

1.4. 공급자는 매년 직원에게 보안 및 개인정보 보호 교육을 제공하고, 모든 직원은 매년 공급자의 행동규약 또는 유사한 문서에 명시된 대로 공급자의 윤리적 비즈니스 행동, 기밀 유지 및 보안 정책을 준수하는지 인증해야 합니다. 공급자는 필수 규정 준수 및 인증 유지에 필요한 경우 서비스, 인도물 또는 Kyndryl 자료의 모든 구성요소에 대한 관리 액세스 권한이 있는 개인에게 추가 정책 및 프로세스 교육을 제공하고, 그러한 개인의 역할 및 서비스, 인도물, Kyndryl 자료의 지원에 적합한 교육을 함께 제공합니다.

1.5. 공급자는 모든 서비스와 인도물 그리고 모든 Kyndryl 기술 핸들링을 위하여 Kyndryl 자료의 가용성을 보호하고 유지 관리하는 보안 및 개인정보 보호 조치들을 설계합니다. 여기에는 설계 단계에서의 보안 및 개인정보 보호, 보안 엔지니어링 및 보안 운영이 요구되는 정책 및 절차의 실행, 유지관리 및 준수를 통한 조치가 포함됩니다.

2. 보안 사고

2.1. 공급자는 컴퓨터 보안 사고 처리에 대한 업계 우수 사례에 따라 문서화된 사고 대응 정책을 유지 관리하고 준수합니다.

2.2. 공급자는 Kyndryl 자료의 무단 액세스 또는 무단 사용을 조사하고 적절한 대응 계획을 정의하고 실행합니다.

2.3. 공급자는 보안 위반을 인지한 후 즉시(그리고 어떤 경우에도 48 시간 이내에) Kyndryl 에 알립니다. 공급자는(이)라는 알림을 cyber.incidents@kyndryl.com 에 제공합니다. 공급자는 Kyndryl 에 그러한 위반 및 공급자의 시정 및 복원 활동 상태에 대한 합리적으로 요청된 정보를 제공합니다. 예를 들어, 합리적으로 요청된 정보에는 디바이스, 시스템 또는 애플리케이션, 관리 및 기타 액세스 권한, 디바이스, 시스템 또는 애플리케이션의 포렌식 이미지 및 기타 유사한 항목을 위반 사항이나 공급자의 시정 및 복원 활동과 관련한 범위 내에서 보여주는 보호된 로그가 포함될 수 있습니다.

2.4. 공급자는 보안 위반과 관련하여 Kyndryl, Kyndryl 계열사 및 고객 (및 그들의 고객 및 계열사)의 모든 법적 의무(규제 기관 또는 데이터 주체에게 알리는 의무 포함)를 충족시키기 위해 합리적인 지원을 Kyndryl 에게 제공합니다.

2.5. 공급자는 Kyndryl 이 서면으로 승인하거나 법에서 요구하는 경우를 제외하고 보안 위반이 Kyndryl 또는 Kyndryl 자료와 직간접적으로 관련되어 있음을 제 3 자에게 알리거나 통지하지 않습니다. 공급자는 법적으로 요구되는 통지를 제 3 자에게 배포하기 전에 Kyndryl 의 신원을 직간접적으로 드러내는 통지를 Kyndryl 에 서면으로 통지합니다.

2.6. 공급자가 본 약관에 의거한 의무를 위반하여 발생한 보안 위반의 경우:

(a) 공급자는 해당 규제 기관, 기타 정부 및 관련 업계 자체 규제 기관, 미디어(해당 법령에서 요구하는 경우), 데이터 주체, 고객 및 기타 개인에게 보안 위반 통지 제공 시 공급자에게 발생하는 비용과 Kyndryl 에게 발생하는 실제 비용을 책임집니다.

(b) Kyndryl 이 요청하는 경우 공급자는 데이터 주체에게 보안 위반을 통지한 날로부터 1 년 동안 또는 관련 정보 보호법에서 요구하는 기간 중 보호 범위가 더 큰 기간 동안 보안 위반 및 관련 결과에 대한 데이터 주체의 문의에 응대하기 위해 자체 경비로 콜 센터를 설립하고 유지합니다. Kyndryl 과 공급자는 협력하여 콜 센터 직원이 문의에 응할 때 사용할 스크립트 및 기타 자료를 작성합니다. 또는, 공급자에 대한 서면 통지에 따라 Kyndryl 은 공급자가 콜 센터를 설립하도록 하는 대신 자체 콜 센터를 설립하고 유지할 수 있습니다. 공급자는 Kyndryl 이 콜 센터를 설립하고 유지하는 것과 관련하여 발생한 실제 비용을 Kyndryl 에 배상합니다.

(c) 공급자는 Kyndryl 이 제공하는 신용 모니터링 및 신용 복원 서비스에 등록하고자 하는, 보안 위반의 영향을 받는 개인에게 보안 위반을 통지한 날로부터 1 년 동안 또는 관련 정보 보호법에서 요구하는 기간 중 보호 범위가 더 큰 기간 동안 그러한 신용 모니터링 및 신용 복원 서비스를 제공하는 것과 관련하여 발생한 실제 비용을 Kyndryl 에 배상합니다.

3. 물리적 보안 및 출입구 통제(아래에서 사용된 대로, "시설"이란 공급자가 Kyndryl 자료를 호스트, 처리 또는 달리 액세스하는 물리적 장소를 의미합니다).

3.1. 공급자는 시설로의 무단 출입을 방지하기 위해 방벽, 카드 제어 출입구, 감시 카메라 및 유인 리셉션 데스크와 같은 적절한 물리적 출입 통제를 유지 관리합니다.

3.2. 공급자는 임시 접근을 포함하여 시설과 시설 내 통제 구역에 대한 접근 승인을 요구하며 직무와 업무적 필요에 따라 접근을 제한합니다. 공급자가 임시 접근 권한을 부여하는 경우 권한이 부여된 직원이 시설 및 통제 구역에 있는 동안 방문자를 안내합니다.

3.3. 공급자는 시설 내 통제 구역으로의 출입을 적절하게 제한하기 위해 업계 우수 사례와 일치하는 다단계 접근 통제를 포함한 물리적 접근 통제를 구현하며 모든 출입 시도를 기록하고 해당 기록을 최소 1 년 동안 보관합니다.

3.4. 공급자는 (a) 승인된 공급자 직원이 퇴사하거나 (b) 승인된 공급자 직원이 더 이상 접근할 유효한 업무상 필요가 없는 경우 시설 및 시설 내 통제 구역에 대한 접근 권한을 취소합니다. 공급자는 접근 통제 목록에서 신속하게 제거하고 물리적 액세스 배지를 반납하는 것을 포함하여 공식 문서화된 퇴사 절차를 따릅니다.

3.5. 공급자는 과도한 주변 온도, 화재, 홍수, 습도, 도난 및 기물 파손과 같은 자연 발생 및 인재로 인한 환경 위협으로부터 서비스, 인도물 및 Kyndryl 기술 핸들링을 지원하는 데 사용되는 모든 물리적 인프라를 보호하기 위해 예방 조치를 취합니다.

4. 액세스, 개입, 전송 및 분리 제어

4.1. 공급자는 서비스 운영, 인도물 제공 및 Kyndryl 기술 핸들링 시 관리하는 네트워크의 문서화된 보안 아키텍처를 유지 관리합니다. 공급자는 해당 네트워크 아키텍처를 별도로 검토하고 시스템, 애플리케이션 및 네트워크 디바이스에 대한 무단 네트워크 연결을 방지하는 방법을 사용하여 안전한 세분화, 격리 및 심층 방어 표준을 준수합니다. 공급자는 호스팅 서비스 호스팅 및 운영에 무선 기술을 사용할 수 없습니다. 그렇지 않으면, 공급자는 서비스와 인도물 제공 및 Kyndryl 기술 핸들링 시 무선 네트워킹 기술을 사용할 수 있지만 그러한 무선 네트워크를 암호화하고 안전한 인증을 요구합니다.

4.2. 공급자는 Kyndryl 자료가 논리적으로 분리되어 권한이 없는 사람에게 노출되거나 그런 사람이 Kyndryl 자료에 액세스하지 못하도록 하기 위한 조치를 유지 관리합니다. 또한

공급자는 자사의 프로덕션, 비 프로덕션 및 기타 환경을 적절히 격리하며, Kyndryl 자료가 비 프로덕션 환경에 이미 존재하거나 이전된 경우(예: 오류 재현 목적으로), 공급자는 비 프로덕션 환경의 보안 및 개인정보 보호가 프로덕션 환경의 보안 및 개인정보 보호와 동일하도록 합니다.

4.3. 공급자는 이동 중이고 (저장 중인 Kyndryl 자료의 암호화가 기술적으로 불가능하다는 사실을 Kyndryl 이 합리적으로 만족할 정도로 입증하지 않는 한) 저장 중인 Kyndryl 자료를 암호화합니다. 또한 공급자는 해당하는 경우, 백업 파일이 포함된 미디어와 같은 모든 물리적 미디어를 암호화합니다. 공급자는 안전한 키 생성, 발급, 배포, 저장, 회전, 취소, 복구, 백업, 파기, 액세스 및 데이터 암호화와 관련한 사용에 대해 문서화된 절차를 유지 관리합니다. 공급자는 그러한 암호화에서 사용된 특정 암호화 방법이 업계 우수 사례(예: NIST SP 800-131a)에 부합하도록 하여야 합니다.

4.4. 공급자는 Kyndryl 자료에 대한 액세스가 필요한 경우 그러한 액세스를 서비스 및 인도물을 제공하고 지원하는 데 필요한 최소 수준으로 제한합니다. 공급자는 기본 구성요소에 대한 관리적 액세스(예: 특권적 액세스)를 포함하여 그러한 액세스는 개별적이고 역할에 근거하며 직무 분리 원칙에 따라 공급자의 권한 있는 직원의 승인 및 정기적인 검증을 받아야 합니다. 공급자는 중복 및 휴면 계정을 식별 및 제거하기 위한 조치를 유지 관리합니다. 또한 공급자는 특권적 액세스 권한을 가진 계정을 해당 계정 소유자의 퇴사 시 또는 Kyndryl 이나 해당 계정 소유자의 관리자와 같은 공급자의 권한 있는 직원의 요청이 있은 이후 24 시간 이내 취소합니다.

4.5. 업계 우수 사례에 따라 공급자는 비활성 세션 시간 초과, 여러 차례의 로그인 실패 후 계정 잠금, 강력한 비밀번호 또는 비밀번호 인증을 강제하는 기술적인 조치와 그러한 비밀번호 및 비밀번호 문구의 안전한 전송 및 저장이 필요한 조치를 유지 관리합니다. 또한 공급자는 Kyndryl 자료에 대한 콘솔 기반이 아닌 모든 특권적 액세스에 대해 다단계 인증을 사용합니다.

4.6. 공급자는 특권적 액세스의 사용을 모니터링하고 (a) 무단 액세스 및 활동 식별, (b) 해당 액세스 및 활동에 대한 적시에 적절한 대응 촉진 및 (3) 공급자, Kyndryl(본 약관의 확인 권리 및 거래서류 또는 당사자들 간의 관련 기본 계약이나 기타 관련성 있는 계약에 의거) 및 기타 기관에서 문서화된 공급자 정책의 준수를 감사하도록 설계된 보안 정보 및 이벤트 관리 조치들을 유지 관리합니다.

4.7. 공급자는 업계 우수 사례에 따라 서비스 또는 인도물의 제공 및 Kyndryl 기술 핸들링에 사용된 시스템에 대한 모든 관리, 사용자 또는 기타 액세스 또는 활동에 대해 기록하는 로그를 보유합니다(요청 시 해당 로그를 Kyndryl 에 제공함). 공급자는 무단 액세스, 수정, 우발적 또는 고의로 그러한 로그를 파기하지 않도록 조치를 유지해야 합니다.

4.8. 공급자는 최종 사용자 시스템을 포함하여 공급자가 소유하거나 관리하고 서비스 또는 인도물의 제공 또는 Kyndryl 기술 핸들링 시 사용하는 시스템에 대한 컴퓨팅 보호를 유지 관리하며 그러한 보호에는 다음이 포함됩니다: 맬웨어 및 고급 지속적 위협을 해결하기 위한 엔드포인트 방화벽, 전체 디스크 암호화, 서명 및 비 서명 기반 엔드포인트 탐지 및 대응 기술, 시간 기반 화면 잠금 및 보안 구성과 패치 요구사항을 적용하는 엔드 포인트 관리 솔루션. 또한 공급자는 알려지고 신뢰할 수 있는 최종 사용자 시스템만 공급자 네트워크를 사용할 수 있도록 기술 및 운영 제어를 구현합니다.

4.9. 업계 우수 사례에 따라 공급자는 침입 탐지 및 예방 및 서비스 거부 공격 대책 및 완화를 포함한 Kyndryl 자료가 존재하거나 처리되는 데이터 센터 환경에 대한 보호를 유지 관리합니다.

5. 서비스 및 시스템 무결성 및 가용성 제어

5.1. 공급자는 다음을 수행합니다: (a) 적어도 1 년마다 보안 및 개인정보 위험 평가를 수행합니다. (b) 서비스 및 인도물에 관련해서는 프로덕션 릴리스 전 및 이후에 매년, 그리고 Kyndryl 기술 핸들링에 관련해서는 매년 자동화 시스템 및 애플리케이션 보안 스캐닝 및 수동 윤리적 해킹을 포함한 보안 테스트를 수행하고 취약성을 평가합니다. (c) 적격한 독립적인

제 3 자에게 최소 매년 업계 우수 사례에 따라 침투 테스트(자동 및 수동 테스트 모두 포함)를 실시하도록 요청합니다. (d) 서비스 및 인도물의 각 구성요소 및 Kyndryl 기술 핸들링과 관련하여 보안 구성 요구사항 준수에 대해 자동화된 관리 및 일상적인 검증을 수행합니다. 및 (e) 관련 위험, 악용 가능성 및 영향을 기준으로 식별된 취약성 또는 보안 구성 미준수 문제를 해결합니다. 공급자는 테스트, 평가, 스캔 및 교정 활동 실행 시 서비스 중단을 피하기 위해 합리적인 조치를 취합니다. Kyndryl 의 요청에 따라, 공급자는 공급자의 최근 침투 테스트 활동에 대한 서면 요약을 Kyndryl 에 제공합니다. 그러한 보고서는 최소한 테스트에서 다룬 오퍼링 이름, 테스트 범위 내 시스템 또는 애플리케이션 수, 테스트 날짜, 테스트에 사용된 방법론 및 경영진을 위한 결과물 요약을 포함합니다.

5.2. 공급자는 서비스, 인도물 또는 Kyndryl 기술 핸들링에 대한 변경사항 적용과 관련된 위험을 관리하기 위해 고안된 정책과 절차를 유지 관리합니다. 영향을 받는 시스템, 네트워크 및 기본 구성요소를 포함하여 변경을 구현하기 전에 공급자는 등록된 변경 요청서에서 (a) 변경에 대한 설명 및 이유, (b) 구현 세부사항 및 일정, (c) 서비스 및 인도물, 서비스 고객 또는 Kyndryl 자료에 대한 영향을 설명하는 위험 설명, (d) 예상 결과, (e) 롤백 계획 및 (f) 공급자의 권한 있는 직원 승인을 기록해야 합니다.

5.3. 공급자는 서비스의 운영, 인도물의 제공 및 Kyndryl 기술 핸들링에 사용하는 모든 IT 자산의 목록을 유지 관리합니다. 공급자는 이러한 IT 자산, 서비스, 인도물 및 Kyndryl 기술(이들의 기본 구성요소 포함)의 상태(용량 포함) 및 가용성을 지속적으로 모니터링하고 관리합니다.

5.4. 공급자는 CIS(Center for Internet Security) 벤치마크와 같이 업계 우수 사례를 충족하는 사전 정의된 시스템 보안 이미지 또는 보안 기준에서 서비스 및 인도물의 개발이나 운영 및 Kyndryl 기술 핸들링에 사용하는 모든 시스템을 구축합니다.

5.5. 비즈니스 연속성과 관련하여 거래서류 또는 당사자들 간의 관련 기본 계약에 따른 공급자의 의무 또는 Kyndryl 의 권리를 제한하지 않고, 공급자는 문서화된 위험 관리 지침에 따라 각 서비스 및 인도물과 Kyndryl 기술 핸들링에 사용된 각 IT 시스템에 대해 비즈니스 및 IT 연속성과 재해 복구 요구사항을 별도로 평가합니다. 공급자는 각 서비스, 인도물 및 IT 시스템이 해당 위험 평가에 의해 보증되는 범위 내에서 비즈니스 및 IT 연속성 및 재해 복구 계획을 업계 우수 사례에 부합하도록 개별적으로 정의, 문서화, 유지 관리 및 매년 검증하였는지 확인합니다. 공급자는 이러한 계획이 아래 5.6 항에 명시된 특정 복구 시간을 제공하도록 설계되는지 확인합니다.

5.6. 호스팅 서비스에 대한 특정 복구 지점 목표("RPO")와 복구 시간 목표("RTO")는 24 시간 RPO 및 24 시간 RTO 입니다. 그럼에도 불구하고, 공급자는 Kyndryl 이 공급자에게 더 짧은 기간의 RPO 또는 RTO 를 서면으로 통지한 후 즉시 Kyndryl 이 고객에게 약속한 RPO 또는 RTO 를 준수합니다(이메일은 서면으로 간주됨). 공급자가 Kyndryl 에게 제공하는 기타 모든 서비스와 관련하여, 공급자는 자사의 비즈니스 연속성과 재해 복구 계획이 공급자가 거래서류 및 당사자들 간의 관련 기본 계약 및 본 약관에 의거 Kyndryl 에 대한 모든 의무를 준수할 수 있도록 RPO 및 RTO 를 제공하도록 설계되어야 합니다. 이러한 의무에는 테스트, 지원 및 유지 관리의 적시 제공이 포함됩니다.

5.7. 공급자는 서비스 및 인도물과 서비스 및 인도물 범위 내의 관련 시스템, 네트워크, 애플리케이션 및 기본 구성요소와 Kyndryl 기술 핸들링에 사용된 시스템, 네트워크, 애플리케이션 및 기본 구성요소에 대한 보안 권고 패치를 평가, 테스트, 및 적용하기 위한 조치를 유지 관리합니다. 보안 권고 패치가 적용 가능하고 적절하다고 판단되면 공급자는 문서화된 심각도 및 위험 평가 지침에 따라 패치를 구현합니다. 공급자의 보안 권고 패치 구현에는 변경 관리 정책이 적용됩니다.

5.8. Kyndryl 이 공급자가 제공하는 하드웨어 또는 소프트웨어에 스파이웨어, 멀웨어, 악성 코드와 같은 침입 요소가 포함되어 있다고 판단할 만한 합리적인 근거가 있는 경우 공급자는 Kyndryl 의 우려사항에 대해 조사하고 시정하는 데 Kyndryl 과 적시에 협력합니다.

6. 서비스 제공

6.1 공급자는 Kyndryl 사용자 또는 고객 계정에 대해 업계 공통의 연합 인증 방법을 지원하며, 공급자는 업계 우수 사례에 따라 (OpenID Connect 또는 Security Assertion Markup Language 를 사용하여 Kyndryl 중앙 관리 다단계 싱글 사인온 등으로) 그러한 Kyndryl 사용자 또는 고객 계정을 인증합니다. 하도급자의 보유와 관련하여, 거래서류 또는 당사자들 간의 관련 기본 계약에 의거한 공급자의 의무 또는 Kyndryl 의 권리를 제한하지 않고 공급자는 공급자에 대한 작업을 수행하는 하도급자가 본 약관에서 공급자에게 적용하는 요구사항과 의무를 준수하는 거버넌스 관리를 도입했는지 확인합니다.

7. **하도급자.** 하도급자의 보유와 관련하여, 거래서류 또는 당사자들간의 관련 기본 계약에 의거한 공급자의 의무 또는 Kyndryl 의 권리를 제한하지 않고 공급자는 공급자에 대한 작업을 수행하는 하도급자가 본 약관에서 공급자에게 적용하는 요구사항과 의무를 준수하는 거버넌스 관리를 도입했는지 확인합니다.

8. **물리적 미디어**. 공급자는 재사용할 물리적 미디어를 재사용 전에 안전하게 소독해야 하며, 미디어 위생에 대한 업계 우수 사례에 따라 재사용할 수 없는 물리적 미디어를 폐기합니다.

제 IX 조, 호스팅 서비스 인증 및 보고서

공급자가 Kyndryl에게 호스팅 서비스를 제공하는 경우 본 조항이 적용됩니다.

1.1 공급자는 아래에 명시된 기간 내에 다음 인증 또는 보고서를 확보합니다.

인증/보고서	기간
공급자의 호스트 서비스와 관련하여: ISO 27001, 정보 기술, 보안 기술, 정보 보안 관리 시스템 준수 인증(신뢰할 수 있는 독립적인 감사자의 평가에 기반한 인증) **또는** SOC 2 Type 2: SOC 2 Type 2에 따라 공급자의 시스템, 제어 및 운영에 대한 검토를 입증하는 신뢰할 수 있는 독립적인 감사자의 보고서(최소한, 보안, 기밀 및 가용성 포함).	공급자는 거래서류의 발효일* 또는 가정 날짜** 이후 120 일까지 ISO 27001 인증을 확보한 후 신뢰할 수 있는 독립적인 감사자의 평가에 기반한 인증을 12 개월마다 갱신합니다(각각의 최신 버전의 표준에 대해 갱신). 공급자는 거래서류의 발효일* 또는 가정한 날짜** 이후 240일까지 SOC 2 Type 2 보고서를 확보한 후, SOC 2 Type 2에 따라 공급자의 시스템, 제어 및 운영에 대한 검토를 입증하는 신뢰할 수 있는 독립적인 감사자의 새 보고서(최소한 보안, 기밀 및 가용성 포함)를 12개월마다 확보합니다. * 발효일 기준으로 공급자가 호스팅 서비스를 제공하는 경우입니다. ** 공급자가 호스팅 서비스를 제공할 의무를 부담하는 날짜입니다.

1.2 공급자가 서면으로 요청하고 Kyndryl 이 서면으로 승인하는 경우, 공급자는 실질적으로 동등한 인증 또는 보고서에 대해서도 위 표의 기간이 변경 없이 적용된다는 점을 조건으로 위에 참조된 것과 실질적으로 동등한 인증 또는 보고서를 확보할 수 있습니다.

1.3 공급자는 다음을 수행합니다: (a) 요청에 따라, 공급자가 확보해야 하는 각 인증 및 보고서의 사본을 Kyndryl 에 즉시 제공하고 (b) SOC 2 또는 실질적으로 동등한 인증(Kyndryl 이 승인한 경우) 검토 중에 언급된 내부 통제 취약점을 즉시 해결합니다.

제 X 조, 협력, 확인 및 시정 조치

공급자가 Kyndryl에게 서비스 또는 인도물을 경우 본 조항이 적용됩니다.

1. 공급자 협력

1.1. Kyndryl 이 서비스 또는 인도물이 사이버 보안 문제의 원인이 되었을 수 있는지, 원인이 되는지 또는 원인이 될 것인지에 대해 질의할 수 있는 경우, 공급자는 문서, 기타 레코드, 관련 공급자 직원 인터뷰 등을 통해서든, 정보 요청에 대해 적시에 완전하게 응대하는 것을 포함하여, 그러한 우려사항에 대한 Kyndryl 의 질의에 합리적으로 협력합니다.

1.2. 당사자들은 다음을 수행하는 데 동의합니다: (a) 요청에 따라 그러한 추가 정보를 상호 제공하고 (b) 그러한 기타 문서를 상호 작성하여 전달하며 (c) 상대방이 본 약관과 본 약관에 언급된 문서의 의도를 이행하기 위해 합리적으로 요청할 수 있는 바대로 기타 조치를 수행합니다. 예를 들어, Kyndryl 이 요청하는 경우, 공급자는 권한 부여의 권리가 있는 경우 계약 자체에 대한 액세스 권한을 부여하는 등, 재처리자 및 하도급자와의 서면 계약에서 개인정보 보호 및 보안 관련 중요한 조항을 적시에 제공합니다.

1.3. Kyndryl 이 요청하는 경우, 공급자는 인도물 및 인도물의 구성요소가 제조되거나 개발되거나 달리 제공된 국가의 정보를 적시에 제공합니다.

2. 확인(아래에서 사용된 대로, "시설"이란 공급자가 Kyndryl 자료를 호스트, 처리 또는 달리 액세스하는 물리적 장소를 의미함)

2.1. 공급자는 본 약관의 준수를 입증하는 감사 가능한 레코드를 유지 관리합니다.

2.2. Kyndryl 은 자체적으로 또는 외부 감사를 통해, 공급자에게 30 일 전에 서면으로 통지하여 본 약관에 대한 공급자의 준수 여부를 확인할 수 있습니다. 준수 확인을 목적으로 시설에 접근할 수 있지만 단, Kyndryl 은 관련 정보를 얻을 수 있다고 판단할 수 있는 정당한 이유가 없으면 Kyndryl 데이터가 처리되는 데이터 센터에 접근하지 않습니다. 공급자는 문서, 기타 레코드, 관련 공급자 직원 인터뷰 등을 통해서든지, 정보 요청에 대해 적시에 완전하게 응대하는 것을 포함하여 Kyndryl 의 확인에 협력합니다. 공급자는 Kyndryl 이 고려할 수 있도록, 승인된 행동규약 또는 업계 인증을 준수한다는 증거를 제공하거나 본 약관의 준수를 입증하는 정보를 제공할 수 있습니다.

2.3. (a) Kyndryl 이 12 개월 기간 동안 기존 확인에서 발견된 우려사항에 대한 공급자의 시정 조치를 검증 중에 있거나 (b) 보안 위반이 발생하여 위반과 관련한 의무 준수를 확인하고자 하는 경우가 아니면 12 개월 기간에 확인은 1 회 이상 수행하지 않습니다. 어느 경우에도 Kyndryl 은 상기 2.2 항에 명시된 대로 동일하게 30 일의 사전 서면 통지를 제공하며, 보안 위반의 해결이 긴급한 경우에는 30 일 미만의 사전 서면 통지로 확인을 수행할 수 있습니다.

2.4. 규제 기관이나 기타 관리자는 규제 기관은 법령에 의거한 추가 권리를 행사할 수 있다는 점을 조건으로 2.2 항 및 2.3 항의 Kyndryl 과 동일한 권리를 행사할 수 있습니다.

2.5. Kyndryl 은 본 약관의 조항을 공급자가 준수하지 않는다고 판단할 수 있는 합리적인 근거가 있는 경우(그러한 근거가 본 약관에 의거한 확인에서 비롯되는지 여부에 관계 없이) 공급자는 해당 미준수를 즉시 시정합니다.

3. 위조 방지 프로그램

3.1. 공급자의 인도물에 전자적 구성요소(예: 하드 디스크 드라이브, SSD, 메모리, 중앙 연산 처리 장치, 논리 디바이스 또는 케이블)가 포함된 경우, 공급자는 1 차적으로, Kyndryl 에 위조 구성요소를 제공하지 못하도록 하고 2 차로, Kyndryl 에 위조 구성요소가 잘못 제공된 경우 이를 즉시 발견하여 정정하도록 하는 문서화된 위조 방지 프로그램을 유지 관리하고

준수합니다. 공급자는 공급자의 인도물에 포함된 전자적 구성요소를 Kyndryl 에 제공하는 모든 공급업체에 대해 문서화된 위조 방지 프로그램을 유지 관리하고 준수하도록 하는 동일한 의무를 부과합니다.

4. 시정 조치

4.1. 공급자가 본 약관에 의거한 의무를 준수하지 않고 이러한 비준수로 인해 보안 위반이 발생한 경우, 공급자는 미이행 사항을 정정하고 보안 위반의 유해한 결과를 시정합니다. 이러한 이행 및 시정은 Kyndryl 의 합리적인 지시와 일정을 따릅니다. 그러나, 공급자의 멀티테넌트 호스팅 서비스 제공으로 인해 보안 위반이 발생하고 결과적으로 Kyndryl 을 포함한 많은 공급자 고객에게 영향을 미치는 경우, 공급자는 보안 위반의 특성을 감안하여 시기적절하고 적절하게 성능 실패를 시정하고 보안 위반의 유해한 영향을 해결하며 이러한 시정 및 문제 해결에 대한 Kyndryl 의 의견을 충분히 고려합니다.

4.2. Kyndryl 은 적절하거나 필요하다고 판단되는 경우 4.1 절에 언급된 모든 보안 위반의 교정 작업에 참여할 권리가 있으며, 공급자는 이러한 보안 위반과 관련하여 당사자가 부담하는 교정 비용 및 지출에 대해 책임을 집니다.

4.3. 예를 들어, 보안 위반 시정 비용 및 경비에는 보안 위반 탐지 및 조사, 관련 법령 및 규정에 따른 책임사항 판단, 위반 알림 제공, 콜 센터 설립과 유지, 신용 모니터링 및 신용 복구 서비스 제공, 정보 재로드, 제품 결함 정정(소스 코드 또는 기타 개발을 통한 방법 포함), 전술한 활동이나 기타 활동을 지원하는 제 3 자 보유, 보안 위반의 유해한 결과를 시정하는 데 필요한 기타 비용 및 경비가 포함될 수 있습니다. 명확하게 하기 위해, 시정 비용 및 경비에는 영업 이익, 사업, 가치, 매출, 영업권 또는 예상 절감이 실현되지 못함으로 인하여 발생하는 Kyndryl 의 손해는 포함되지 않습니다.