

CITI 공급업체 요건

책임자:
Citi 구매 및 리스크 책임자

발행일:
2015 년 1 월

수정일:
2026 년 9 월

버전:
9

목차

1	개관	3
2	평등 고용 기회	4
3	뇌물수수 및 부패 방지(AB&C)	5
4	선물 및 향응	6
5	공급업체 관리 및 공급업체 원칙	6
6	현대판 노예 제도 금지	7
7	공급업체 직원	9
8	사기 관리	10
9	미디어 접촉 및 홍보 출연	11
10	서면 전자 통신	12
11	정치 활동 및 기부금	13
12	자금세탁방지(“AML”)	13
13	기록 관리	15
14	기업 복원력/사업 연속성	16
15	글로벌 신원조회 기준	22
16	비용	24
17	정보 보안(IS)	25
18	보안 작업장 지침	60
19	인공 지능/머신 러닝(생성형 AI/에이전트형 AI 포함)	61
20	고객 불만	62
21	개인 거래 및 투자 정책	63
22	청구 및 송장 표준	63
23	의무 휴가 정책	64
	부록 - 정의	65

1 개관

1.1. 일반 요건

이 Citi 의 공급업체 요건(“요건”)에서는 공급업체가 Citi 와 비즈니스를 수행하는 과정에서 반드시 충족해야 하는 몇 가지 의무에 대해 자세히 설명합니다. 일부 요건은 모든 공급업체에 적용되지만, 특정 공급업체에 대한 기타 요건의 적용 여부는 해당 공급업체가 Citi 에 제공하는 제품 및 서비스 유형에 따라 다릅니다(후자는 아래 섹션 1.2 에 요약되어 있으며, 이 섹션의 각 조항 시작 부분에 표시되어 있음). 대문자로 표시된 용어는 이 문서에서 별도로 명시한 의미가 없는 한, 이 문서(첨부된 부록 포함)에 부여된 의미를 가집니다. 이 문서에서 별도로 명시한 대문자 용어는 아래에 정의한 바와 같이 계약서에 명시된 의미를 지닐 것입니다.

이러한 요건들은 Citi 와의 공급업체 계약서(거래 문서, 예를 들어 작업 발주, 라이선스 일정을 포함하되 이에 국한되지 않음)(각각 '계약서')에 따른 계약상 의무이며, 모든 계약서에 명시된 의무, 관련 법률에 따른 의무(해당 용어는 아래에 정의됨), Citi 가 공급업체에 계약서에 명시된 의무에 따라 의무를 알리는 통지서(각각 '통지서'), 또는 Citi 의 비즈니스나 업무 부서가 도입한 보다 구체적인 추가 요건 충족 의무 외에 추가로 적용되는 요건들입니다. 전술한 요건과 이러한 요건이 충돌하는 경우, 더 강력한 제한이 적용되는 의무와 요건이 우선순위를 갖게 됩니다. 공급업체는 규정 준수를 보장하기 위해 이러한 요건과 관련하여 궁금한 점이 있을 경우, 반드시 적극적으로 궁금한 점에 관하여 자사의 Citi 비즈니스 담당자(또는 위임자)에게 문의해 파악할 책임이 있습니다. 여기에는 해당 요건의 변경, 일체의 요건 면제 요청, 또는 그러한 요건 간의 불일치나 관련법과의 불일치가 포함됩니다.

공급업체는 Citi 가 관련 법률을 준수해야 하는 Citi 의 의무와 관련된 공급업체 서비스 또는 직원과 관련하여 요구하는 데이터에 대해 Citi 가 공급업체에 제기할 수 있는 합리적인 요청을 즉시 준수해야 합니다. 공급업체가 이러한 의무를 준수하지 못하는 경우 본 계약 조건의 중대한 위반으로 간주됩니다.

이러한 계약 요건을 준수하지 못하거나, Citi 사업부가 지정한 일체 추가 요건을 준수하지 못할 경우 공급업체와 Citi 간의 계약이 해지될 수 있습니다. 더욱이, '요건'의 위반은 관련 법률 위반이 될 수도 있으며, Citi(또는 제 3 자)에 민사상 손해를 초래하거나 공급업체가 형사 처벌을 받을 수도 있습니다. 공급업체는 Citi 의 서면 동의 없이 이러한 계약 요건 조항을 준수할 의무를 자사 정책 준수로 대체할 수 없습니다.

1.2. 일부 공급업체에 적용되는 요건

다음 표는 해당 표에 명시된 적용 기준을 충족하는 특정 공급업체에 적용되는 특정 요건을 나열한 것입니다. 아래에 언급되지 않은 섹션은 모든 공급업체에 적용됩니다.

섹션 #	섹션 제목	적용대상
2	평등 고용 기회/소수 집단 우대 정책	미국 연방 정부와의 Citi 계약 이행에 필요한 계약 및 구매 주문에 적용됩니다. 계약 또는 구매 주문이 연방 정부 하도급계약 또는 구매 주문에 해당하는지 불확실한 경우에는 적절히 조항의 처음 또는 끝에 ‘해당하는 경우’를 포함하십시오.

섹션 #	섹션 제목	적용대상
12	자금세탁방지	특정 고객 관련 서비스(예: 온보딩, 고객 계좌 및 거래 심사) 또는 이러한 활동에 관련된 데이터/메트릭 전송을 수행하는 공급업체, 및/또는 현금 또는 금융 수단(예: 원격 입금 캡처, 배달원, 현금수송용 무장 차량 또는 록박스(lockbox) 서비스) 관련 중개인 역할을 하는 공급업체에 적용됨.
13	기록 관리	*Citi 정보의 액세스/처리/저장 서비스를 제공하는 공급업체에 적용됨
14	사업 연속성	Citi 가 사용하는 서비스 또는 호스트 기술 인프라/애플리케이션을 제공하는 공급업체에 적용됩니다. Citi Business Activity Owner(BAO)는 이러한 요건의 적용 가능성과 COB 요건을 해당 공급업체에 알려야 할 책임이 있습니다.
15	글로벌 신원조회 기준	Citi 에 서비스를 제공하는 공급업체에 적용됩니다.
16	비용	계약상 상환 가능한 사업 비용을 청구할 자격이 있는 공급업체에 적용됩니다.
17	정보 보안(IS)	Citi 정보에 액세스하거나 이를 처리, 관리 또는 저장하는 하청업체를 포함한 공급업체에 적용됩니다. 그리고/또는, Citi 브랜드의 인터넷 응대 애플리케이션을 위해 호스트 역할을 담당하는 공급업체, 그리고/또는 Citi 의 네트워크 리소스에 연결된 공급업체, 그리고/또는 Citi 시설에 동반자 없이 액세스가 필요한 공급업체에 적용됩니다.
18	보안 작업장 지침	
19	인공 지능/머신 러닝(생성형 AI/에이전트형 AI 포함)	제공하는 상품/서비스의 어느 부분에서든 Citi 가 정의한 인공지능/머신 러닝(AI/ML)을 활용하는 공급업체에 적용됩니다.
20	개인 거래 및 투자 정책	Citi 에서의 직무의 일환으로 MNPI 에 정기적으로 액세스해야 하는 공급업체에 적용.
23	의무 휴가 정책	본 정책은 민감한 직책(용어집에 정의됨)을 맡은 비직원('근로자')('민감 직책 근로자')과 민감 직책 직원의 직속 관리자 및 감독자('관리자'), 민감 직책 비직원의 Citi 비즈니스 담당자에게 적용됩니다.

2 평등 고용 기회

2.1 평등 고용 기회.

Citi 는 인종, 피부색, 종교, 성별, 성적 취향, 성 정체성, 출신 국가, 시민권, 이민 상태, 나이, 결혼 상태, 유전 정보, 장애, 보호받는 재향군인 지위 또는 법으로 보호되는 기타 특성과 무관하게 자격을 갖춘 모든 사람에게 평등한 고용 기회를 보장하도록 설계된 정책을 개발했습니다.

공급업체는 Citi 가 서면으로 준수 의무를 통지한 그러한 법 서면으로 공급업체에 통지하는 차별 금지 법률이나 규정을 포함하되 그에 국한되지 않는 모든 적용 가능한 그러한 법률 및 규정의 요건을 준수하고, 자사 직원이 함께 그러한 요건을 준수하도록 조치해야 합니다.

공급업체는 Citi 의 미국 평등고용기회정책 선언문(www.citigroup.com/global/eeo-aa-policy 에서 확인 가능)을 검토하고 이에 따라 적절한 조치를 취해야 합니다.

2.2 정부 계약

연방 정부와 Citi 계약을 이행하는 데 필요한 계약 및 구매 주문서에는 아래에 표시된 대로 굵은 글씨로 다음 조항을 그대로 포함해야 합니다. (연방 정부 하청 계약/구매 주문인지 확실하지 않은 경우, 해당 섹션의 시작 부분에 "해당되는 경우"를 포함하여 추가합니다.)

[해당되는 경우,] 공급업체는 모든 해당 연방 차별 금지 법률을 준수하고 해당 연방 차별 금지 법률을 위반하는 프로그램을 운영하지 않음을 증명합니다.

2.3 정부 계약 부록

연방 정부와 Citi 계약을 이행하는 데 필요한 계약 및 구매 주문서는 하청 계약 또는 구매 주문서 부록에 다음 통지 사항을 포함해야 합니다. (연방 정부 하청 계약/구매 주문인지 확실하지 않은 경우 아래 통지의 끝에 "해당되는 경우"를 포함하여 추가합니다.)

연방 정부 계약업체로서, Citigroup 은 보호 대상 재향군인 및 장애인을 대신하여 서명한 계약업체 또는 공급업체에 평등 고용 기회 의무를 서면으로 통지합니다. Citigroup 은 재활법 제 503 조 및 베트남 전쟁 참전 용사 재조정 지원법과 각각 41 C.F.R. § 60-741 및 41 C.F.R. § 60-300 에 따른 해당 규정을 완전히 준수합니다. 당사의 평등고용기회정책 선언문은 www.citigroup.com/global/eeo-aa-policy 에서 확인할 수 있습니다. 당사의 EEO 정책 선언문에 대한 문의 사항은 정책 선언문에 제공된 연락처로 문의하시기 바랍니다.

[해당되는 경우], 당사 정책 선언문 및 규정에 따라 적절한 조치를 취해주시기를 요청드립니다.

3 뇌물수수 및 부패 방지(AB&C)

Citi 는 적용 가능한 AB&C 법률을 준수하도록 합리적으로 설계된 정책, 절차 및 내부 통제를 갖추고 있으며, 어떠한 형태로든 뇌물수수나 급행료 지불을 엄격히 금지합니다. 공급업체(비즈니스 중개인 포함), 그 직원 또는 Citi 를 대신하여 직간접적으로 행동하는 모든 사람은 가장 높은 윤리 기준에 따라 활동을 수행해야 하며, 미국 해외 부패 행위 방지법(FCPA), 영국 뇌물 방지법(UKBA) 및 각각 개정된 법률, 그리고 Citi 가 운영되는 국가의 모든 기타 해당 현지 AB&C 법률을 준수해야 합니다.

공급업체 또는 Citi 를 대신하여 운영하거나 공급업체와 Citi 간의 계약 또는 관계와 관련된 공급업체의 직원은 (i) 어떠한 사람에게도 지급금, 혜택, 이권 또는 기타 가치 있는 것을 제공, 허가 또는 제안하지 않으며 (ii) FCPA, UKBA 또는 기타 AB&C 법률을 위반하여 (i)-(ii)의 각 사례에서 어떤 사람에게서든 지급금, 혜택, 이권 또는 기타 가치 있는 것을 받거나 수락하지 않습니다. 공급업체와 그 직원은 Citi 를 대신하여 또는 공급업체와 Citi 간의 계약 또는 관계와 관련하여 이 섹션 포함한 요건을 준수하여 활동 및 거래를 수행해야 합니다. 또한 공급업체와 그 직원은 AB&C 준수 프로그램을 유지 관리해야 하며, 모든 AB&C 법률을 준수하도록 설계 및 적용된 정책과 절차도 유지해야 합니다.

Citi 의 AB&C 프로그램에 대한 개요는 [Citigroup Investor Relations\(IR\)](#) 페이지에서 확인하십시오(Citi 정책 아래에서 AB&C 프로그램을 선택).

4 선물 및 향응

공급업체와 그 직원은 Citi 직원에게 선물이나 가치 있는 것(향응 포함)을 제공할 수 없습니다. 이는 선물이나 가치 있는 것을 제공할 경우 실제적 또는 표면적 이해 상충이나 상호 이익이 발생하거나 직원의 무결성이나 판단력이 손상되거나 직원의 의사 결정에 부당한 영향을 미치거나 직원이 자신의 의무에 반하는 행동을 하게 하거나 해당 법률을 위반하는 행위가 될 수 있기 때문입니다. 앞서 언급한 것에 국한되지 않고, 직원은 G&E 표준의 금지된 선물 및 접대 섹션을 준수해야 합니다. 공급업체와 그 직원은 Citi 직원에게 1 년에 한 사람당 총액이 미화 300 불을 초과하는 비현금성 비즈니스 선물을 제공해서는 안 됩니다.

공급업체가 Citi 직원에게 비즈니스 향응(예: 식사, 스포츠, 문화 또는 기타 유사한 행사에의 초대)을 제공하는 경우, 공급업체는 해당 행사에 참석해야 하며 향응은 적절하고 관례적이며 합리적이어야 하며 호화롭거나 지나치게 빈번해서는 안 됩니다. 또한 공급업체가 행사에 참석하지 않을 경우, 해당 접대는 업무상 선물로 간주되며, Citi 선물 및 접대 표준이 적용되는 보고 기준에 따라 처리됩니다. 공급업체는 부패나 부적절하거나 해당 법률을 위반한 것으로 간주되거나 합리적으로 그렇게 인식될 수 있는 경우 Citi 를 대신해 또는 Citi 를 대신하는 것처럼 가장하여 공급업체의 비용이나 Citi 직원의 비용을 포함하여 어떠한 대가도 직접 또는 간접적으로 누구에게도 제공해서는 안 되며, 타인이 그러한 행위를 하도록 유도해서도 안 됩니다.

5 공급업체 관리 및 공급업체 원칙

<https://www.citigroup.com/citi/suppliers/> Citi 는 다양한 이니셔티브를 위해 공급업체와 협력하고, 당사가 서비스를 제공하는 지역사회에 잠재적 공급업체를 대상으로 Citi 의 조달 프로그램에 대한 인식을 높입니다. 또한 이러한 협력 활동은 특히 새롭게 대두되는 비즈니스 문제를 해결하기 위한 혁신적인 솔루션을 추진하는 유망

공급업체를 발굴하는 것을 목적으로 합니다. 공급업체에 대한 Citi의 기대 사항에 대한 추가 정보는 [Doing Business with Citi](#) 사이트에서 확인하실 수 있습니다.

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

6 현대판 노예 제도 금지

Citi는 현대판 노예제 및 인신매매가 자사 조직이나 공급망 내에서 발생할 수 있는 리스크를 식별하고 이를 예방하기 위한 관행을 유지하기 위해 최선을 다하고 있습니다. Citi의 공급업체는 아래에 명시된 요건을 준수하고 자체 운영 및 공급망 내에서 현대판 노예 및 인신매매 리스크를 식별하고 예방하기 위해 효과적인 전사적 정책, 절차 및/또는 관행을 개발해야 합니다. 공급업체는 Citi가 특히 고위험 부문·지역 소재 공급업체에 대해 리스크 노출과 잠재적 경감 절차를 평가할 수 있도록 필요한 추가 정보를 포함하여 Citi가 요청한 대로 Citi의 기업 책임 설문지를 작성해야 합니다. 공급업체의 하청업체도 동일한 프로세스를 따라야 합니다.

6.1 아동 노동 방지

공급업체는 아동 노동자를 고용해서는 안 됩니다. ‘아동’이란 적용 법률상 최저 고용 연령 미만인 사람 또는 그러한 법률이 없는 경우 15세 미만이거나 의무교육 이수 연령 미만인 사람 중 더 높은 연령 기준에 해당하는 사람을 의미합니다. 아동 노동에 대한 포괄적인 금지 원칙을 전제로, 만약 18세 미만의 근로자가 고용될 경우, 그들이 수행하는 업무와 근무 환경에 대해 각별한 주의가 기울여져야 하며, 이는 근로 또는 근로 조건으로 인해 신체적, 정신적 또는 기타 어떤 해도 입지 않도록 하기 위함입니다.

6.2 자발적 근로

공급업체는 근로자가 정신적·육체적으로 강압을 받아 구속 억류 노동 또는 도제계약 노동을 강요받거나, 강제 초과 근무를 포함한 어떠한 형태로든 비자발적인 죄수 노동, 노예 매매 또는 강제 노동의 대상이 되는 일이 없도록 보장해야 합니다. 모든 근로는 반드시 자발적으로 수행되어야 합니다. 이 문서에 따른 공급업체의 의무에는 다음 사항을 보장하는 것이 포함되며 이에 국한되지 않습니다.

1. **계약, 임금 및 근무 시간:** 근로자에게는 고용 조건을 명시한 서면 문서가 제공되어야 합니다. 이 문서는 쉽게 이해할 수 있도록 작성되어야 하며, 근로자의 권리와 의무가 명기되어야 합니다. 이 서면 문서에는 임금, 초과근무 수당, 지불 기간, 근로 시간, 휴식 및 휴일과 관련된 권리에 대한 투명한 조건이 포함되어야 하되 이에만 국한되지는 않습니다. 이와 같이 서면으로 작성된 근무 조건은 근로자가 업무를 시작하기 전에 제공되어야 하고, 고용주는 이 조건을 따라야 하며, 산업 기준, 그리고 업무 수행과 관련된 법률 및 단체 협약의 최소 요건을 충족해야 합니다.

2. **자유롭게 직장을 그만둘 수 있는 권리:** 근로자는 적용 가능한 법률 및 단체협약에 따라 합리적인 기간의 통지를 거쳐 자유롭게 고용을 종료할 권리가 있어야 하며, 부적절한 처벌이 부과되지 않아야 합니다.
3. **비인도적인 대우:** 근로자, 그 가족 및 이들과 밀접한 관련이 있는 사람들은 육체적 처벌, 육체적, 정신적 또는 성적 폭력이나 강요, 언어 폭력, 괴롭힘 또는 협박을 포함하되 이에 국한되지 않는 가혹하거나 비인도적인 대우를 받아서는 안 됩니다. 이주 노동자와 그 가족, 그리고 그들과 밀접한 관계가 있는 사람들은 국적을 이유로 근무 조건에 있어 차별을 받아서는 안 됩니다.
4. **임금, 복지 및 근무 시간:** 보상은 최저 임금, 초과근무 수당 및 법에서 규정하는 복지 혜택을 포함한 모든 관련 임금 법률을 준수해야 합니다. 직원에게는 급여를 전액, 제때 지급하고 투명성 있는 급여 명세서를 제공해야 합니다. 징계 조치로서 임금 또는 복리후생을 벌칙성으로 공제하거나 지급을 보류해서는 안 됩니다. 주당 근무 시간은 현지 법률에서 정한 최대 시간을 초과해서는 안 되며, 초과근무는 자발적으로 이루어져야 하고 법정 한도 내에서 시행되어야 하며, 초과근무를 거부했다는 이유로 처벌해서는 안 됩니다.
5. **신분증 압수 금지:** 근로자의 신분증, 여행 허가증, 여권 또는 기타 공식 문서나 기타 귀중품은 고용 조건으로 압수되거나 보류되어서는 안 되며, 재산의 보류는 근로자의 자유를 제한하거나 직장 내 노예제도를 조성하는 데 직접 또는 간접적으로 사용되어서는 안 됩니다.
6. **채용 수수료나 채무 속박 금지:** 근로자 채용과 관련된 수수료나 비용(취업 비자, 여행 경비 및 문서 처리 비용이 포함되나 이에만 국한되지 않음)을 직접적으로나 간접적으로 근로자에게 부과해서는 안 됩니다. 이와 마찬가지로, 담보 제공을 포함하여 직장 내 노예 노동을 유도할 의도가 있거나 이런 효과를 가지는 지불을 하도록 근로자에게 요구하거나, 일을 통해 채무를 갚도록 근로자에게 요구해서는 안 됩니다. 채용 과정과 관련하여 근로자에게 수수료 또는 비용이 부과되었거나 고용 기간 중 그러한 비용이 발생한 것으로 확인되는 경우, 공급업체는 해당 비용이 신속히 환급되도록 합리적인 조치를 취해야 합니다. 직업 소개소와 같은 제 3 자를 통해 근로자를 채용해야 하는 경우, 평판이 좋은 직업 소개소만 이용해야 합니다. 직접 고용을 위해 근로자 채용을 외주하는 경우, 평판이 좋은 취업 알선 업체만 이용해야 합니다. 근로자 부담 채용 수수료 금지는 모든 채용 담당자, 대리인, 하위 대리인에게 적용됩니다. 공급업체는 준수를 보장하기 위한 통제 수단을 마련해야 합니다. **이동의 자유:** 근로자는 불합리한 제한 없이 자유롭게 이동할 수 있어야 하며, 직장이나 고용주가 통제하는 다른 장소(예: 숙소 건물)에 물리적으로 갇혀서는 안 됩니다. 수행하는 업무의 위치나 특성 때문에 필요한 경우를 제외하고, 근로자에게 고용주가 통제하는 구내에 숙소를 잡도록 요구해서는 안 됩니다.

7. **보복이 따르지 않는 불만 제기:** 근로자는 고용주의 처우에 대해 자유로이 고용주에게 불만을 제기할 수 있어야 하며, 불만을 제기한 것 때문에 손해, 보복 또는 피해를 당해서는 안 됩니다.

7 공급업체 직원

7.1 공급업체 직원 교육, 업무 배정, 업무 재배정 및 관리.

공급업체는 일체의 계약 내용에 준하는 가장 효과적인 방식으로 서비스를 수행하기 위해 적절한 훈련, 교육, 경력, 기술을 갖춘 적절한 인원의 개인을 투입하고 그러한 개인들의 자격을 입증할 자료를 갖춰야 합니다. 인력이 특정 프로젝트에 배정된 이후에는 Citi의 사전 서면 동의 없이 해당 인력을 다른 업무에 재배치하거나 프로젝트에 투입 가능한 시간을 줄이는 방식으로 활용해서는 안 되며, 프로젝트 수행 시 재적응으로 인한 혼선을 최소화할 수 있도록 인력을 배정해야 합니다. 공급업체는 자사 인력이 Citi의 직원이나 대리인인 것처럼 행세하거나, Citi로부터 제공되는 복리후생, 장애 소득, 사회보장세 또는 급여, 연방 실업세, 주 실업 보험 혜택, 연방 소득세 원천징수 등과 관련하여 Citi의 직원으로 대우받으려 해서는 안 되도록 해야 합니다. 공급업체는 자사 직원과 관련하여 모든 고용 관련 의무와 관련하여 전적인 책임을 집니다. 여기에는 필수 보험 보장, 독립 계약자인 공급업체로서 지니는 의무에 준하는 형태로 모든 세금 보고서 신고 및 세금 납부·예납과 같은 의무를 완수하는 것이 포함됩니다(이에 국한되지 않음).

7.2 공급업체 직원 교체

공급업체 측이 특정 프로젝트에 배정한 일체의 직원을 Citi가 차별적이지 않은 이유로 수용할 수 없다고 통보할 경우, 공급업체는 해당 직원을 프로젝트에서 배제하고 교체해야 합니다. 또한 공급업체는 배정된 직원이 적시에 전문가다운 태도를 갖고 맡은 서비스 업무를 수행할 수 없거나 수행할 의사가 없는 경우, 즉시 프로젝트에 배정된 직원을 배제하고 교체할 것과 해당 직원이 Citi에 서비스(또는 Citi 서비스 업무 수행이나 감독 업무와 관련된 모든 업무)를 제공하는 업무를 담당하지 못하도록 한다는 데 동의합니다.

7.3 공급업체 직원 정책

공급업체는 Citi에 현장 서비스 업무를 담당하도록 배정한 자연인인 자사 직원의 자격을 확인하는 데 필요한 포괄적인 정책 및 절차를 유지하고 효과적으로 관리하고 있는 동시에 그러한 정책과 절차에는 관련 법률 및 해당 단체 교섭 협약이 허용하는 범위 내에서 근로 허가 확인, 고용 기록 및 범죄 전과에 대한 신원 조회(본 문서에 추가로 명시됨), 고용 전 약물 검사가 포함되어 있음을 이로써 진술하고 보증하고 약정합니다. 앞서 언급한 일반 사항을 제한하지 않는 범위 내에서, 공급업체는 이민 관련 적용 법률을 완전히 준수하기 위한 통제 및 절차를 갖추고 있으며, Citi에 배정된 모든 인력이 과제 기간 동안 해당 이민 관련 법률을 완전히 준수한 상태로 근무할 수 있는 자격을 갖추었음을 확인했음을 진술하고 보증하며 이를 지속적으로 준수할 것을 약속합니다. 요청 시 공급업체는 Citi에 배정된 일부 또는 모든 공급업체 직원에 대한 노동 허가 및 이민 관련 준거법 준수를 입증하는 증빙 자료를 Citi에 즉시 제출해야 하며, 관련 법률상 작업 허가를 받지 않은 직원이 있으면, 절한 자격을 갖춘 대체 인력으로 교체해야 합니다. 이러한 인력 교체는

각 사례마다 Citi의 추가 비용 없이 적시에 효과적인 서비스 제공을 보장하는 데 필요한 모든 교육 및 오리엔테이션 교육을 실시하는 것도 포함됩니다.

7.4 공급업체 소유권

Citi가 사업을 수행하는 관할지역의 해당 법률 및 규정을 준수하기 위해 Citi의 요청에 따라 공급업체는 소유자의 세부 정보를 제공할 의무가 있습니다. 소유자는 자연인 및/또는 법인이며, 여기에는 공급업체의 직접 소유자부터 영향을 미치거나 다른 수단을 통해 계약, 제품 또는 서비스에 대한 직간접적 소유권 또는 통제권을 갖는 최종 실질 소유자까지 포함됩니다.

8 사기 관리

사기 리스크("사기 관리")를 식별하여 경감하려는 Citi의 노력 관련

8.1 모든 공급업체는,

1. 의심스럽거나 혐의가 있는 절도, 사기나 기타 잠재적인 범죄 행위나 불법 행위에 대한 Citi의 모든 조사 및 사기·범죄 행위의 기소와 관련하여 법이 허용하는 최대한의 범위에서 협력해야 합니다.
2. [Ethics Hotline](#)을 통해 잠재적인 사기 사건을 적시에 Citi에 보고하고 회부합니다. 여기에는 Citi, Citi 직원, Citi 공급업체나 대리인 또는 비 Citi 직원(예: 임시 직원 및 계약 직원)이 시도하였거나, 의심을 받거나, 혐의가 있는 행위, 또는 실제로 벌어진 절도, 사기(예: 거짓임을 알면서도 공급업체에 대해 부정확하거나 허위인 데이터를 제출하는 것, 청구 사기, 자금이나 증권 의 소실), 범죄행위 또는 불법행위가 포함되며, 이에만 국한되지 않습니다.
3. Citi 및 그 대표자의 모니터링과 감독을 허용하고, 해당 공급업체와 관련된 잠재적인 사기 행위에 대해 Citi 및 법 집행당국이 주도하는 조사를 지원합니다.
4. 공급업체가 알게 된 이해 상충(공급업체/공급업체 직원 및/또는 Citi 직원 간의 이해 상충 포함)을 적시에 보고하고,
5. Citi의 공급업체 결제 시스템에서 공급업체의 은행계좌를 설정하거나 업데이트하는 과정에서 Citi의 사기 방지 프로세스를 지원해야 합니다.

8.2 이에 더하여, 본질적으로 사기 리스크가 높은 서비스를 제공하는 공급업체는 다음을 **필히** 수행해야 합니다.

1. 공급업체에서 Citi에 제공하는 서비스에 관련된 사기 리스크를 실제로 구분할 수 있는 '사기 리스크 관리 프로그램'을 기록하고 후속 조치를 할 것. 그리고 이러한 리스크를 관리하고 경감시킬 수 있는 과정을 실행할 것
2. 사기 인식 교육을 완료하고(고용 후 90일 이내 및 그 이후 매년) Citi에 제공되는 특정 서비스와 관련된 사기 위험의 특정 요소에 대해 직원을 교육할 것

3. 사기 시도가 이루어진 사건들을 모니터링하고, Citi 에 제공하는 서비스와 관련된 사기 리스크를 경감시키기 위해 효율적인 관리체계를 유지하고, 관리 절차를 문서로 기록하고 지속적으로 관리 효율성을 테스트하며, 모든 하자를 사업활동소유주(BAO)에게 보고할 것
4. Business Activity Owner(BAO)에 대한 사기 위험 노출의 실사/지속적인 모니터링/평가를 위해 필요한 정보를 제공할 것
5. 실사에는 공급업체의 사기 위험 완화 역량에 대한 통제 평가를 수행하도록 설계된 제 3 자 사기 영향 평가 템플릿(Third-Party Fraud Impact Assessment Template, TP-FIAT)이 포함됩니다. 이 운영 절차는 사기 리스크를 식별하고 관리하기 위해 Business Activity Owner(BAO) 또는 Third-Party Officer(TPO)와 Fraud Risk Management Officer(FRMO)가 수행할 일련의 단계를 설명합니다.

8.3 본질적으로 사기 리스크가 높은 공급업체는 다음을 포함하되 이에만 국한되지는 않습니다.

1. Citi 의 직접적인 통제나 감독을 받지 않는 상태에서 내부 계좌 접근, 금융 거래, 현금 거래 등 사기 행위를 가능하게 하는 데 사용될 수 있는 기밀 등급 이상으로 분류된 데이터에 접근할 수 있는 경우.
2. Citi 네트워크/시스템에 접속할 수 있는 경우, 그리고
3. 다음을 포함하여 사기를 저지르거나 가능하게 하는 데 타깃이 될 수 있는 서비스 및 역량을 제공, 지원 또는 접근하는 경우:
 - a) 신원확인, 온보딩, 신규 고객의 신청서 처리
 - b) Citi 또는 고객 결제/자금 이체 활동 및/또는 Citi 고객이 이러한 서비스에 접근할 때의 인증 절차
 - c) Citi 데이터 또는 Citi 고객 데이터(예: 인구 통계)를 만들거나, 확인하거나, 변경하는 것
 - d) 거래 수단(예: 직불/신용 카드, 전자지갑, 체크북 등)의 제공, 서비스 또는 인증
 - e) Citi 의 사기 예방, 감지 또는 사기 활동 발생 시 대응하는 것과 관련해 Citi 에 운영상 사기 관리 활동을 제공하거나 지원하는 것
 - f) 현금, 금융 상품 및 자산/물리적 상품에 대한 물리적 접근 제공
 - g) Citi 시설에 동반인 없이 또는 업무시간 이후에도 접근 가능
 - h) 재무제표: GL/SL 에 항목을 게시하는 것과 같은 회계 활동
 - i) 인센티브 활동 관련 보상 소득 및 지출.

9 미디어 접촉 및 홍보 출연

Citi 기업 서비스와 홍보부(Enterprise Services and Public Affairs)는 Citi 를 대신하여 보도자료 또는 공개성명을 발표할 권한이 있는 유일한 부서입니다. 공급업체는 Citi,

공급업체와 Citi 간의 계약이나 합의 또는 Citi 가 공급업체로부터 조달하는 제품과 서비스를 직접 또는 간접적으로 밝히는 보도자료를 발행할 수 없습니다. 공급업체는 각 Citi 의 BSRM 또는 Citi 의 주 비즈니스 담당자의 사전 서면 승인 없이 Citi 고객, Citi 직원, 여타 Citi 공급업체, 공급업체의 다른 고객 또는 기타 제 3 자와 관련된 일체의 홍보 활동에 동의하거나 관여해서는 안 됩니다.

공급업체는 각 Citi BSRM 또는 Citi 의 주 비즈니스 담당자나 국가 홍보 담당 고위 임원의 사전 서면 승인 없이 서면 또는 전자 형식으로 (서적, 기사, 팟캐스트, 웹캐스트, 블로그, 웹사이트 포스팅, 사진, 비디오, 소셜 미디어 또는 기타 매체를 포함하여) Citi, Citi 의 업무, 고객, 제품 또는 서비스를 언급하는 자료를 발표 또는 게시하거나, 연설하거나, 인터뷰하거나 대중적으로 공개해서는 안 됩니다.

Citi 에 대한 서비스나 제품의 공급과 상관없이 공급업체는 각각의 경우에 있어서 Citi 의 사전 서면 승인을 확보하지 않고 Citi 의 고유 표시, 상표, 서비스 표시, 거래 명칭, 로고, 상징 또는 브랜드 명칭을 사용해서는 안 됩니다. 공급업체는 Citi 외부에서 이익을 위하여 또는 업무를 위하여 Citi 의 명칭, 로고 또는 상표, 시설 또는 관계(레터헤드 또는 개인용 웹사이트, 블로그 또는 다른 소셜 네트워킹 사이트를 포함하여)를 사용해서는 안 됩니다. 나아가 공급업체는 자선 또는 무료 서비스의 목적을 위해 Citi 의 명칭, 시설 또는 관계를 이용해서는 안 됩니다.

10 서면 전자 통신

Citi 직원과 교류하거나 Citi 를 위하여, 또는 Citi 를 대신하여 자사의 의무를 수행할 때, 공급업체는 Citi 가 승인한 서면 전자 통신 장비, 시스템 및 서비스만 사용할 수 있습니다. 독립형 도구든, 아니면 보다 넓은 플랫폼에 통합되었든, Citi 가 제공한 것이든, 제 3 자가 제공한 것이든 상관 없이 신규, 확장 또는 수정된 Citi eComm 채널은 BAO 가 서면으로 공급업체에 통지한 해당 Citi 요건에 따라 승인받아야 합니다. WhatsApp, WeChat, LINE, Slack, Signal, Telegram, iMessage, SMS, Viber 및 기타 대화형 전자 플랫폼과 같이 Citi 가 승인하지 않은 메시징 플랫폼에서 Citi 직원과 Citi 비즈니스에 관한 정보를 주고받는 것을 금지합니다.

또한, 공급업체는 Citi 가 제공한 통신 장비, 시스템 및 서비스를 통해 생성, 발견, 사용, 액세스, 다운로드, 저장, 전송, 수신 또는 삭제된 서면 전자 통신에서 주고받은 개인정보가 보호될 것으로 기 대해서는 안 됩니다. Citi 는 전자 통신 장비, 시스템 및 서비스, 전자 통신을 모니터링할 수 있습니다. 그러한 전자 통신은 Citi 가 소유하며, 해당 기록의 보존 요건(현지 법률 및 규정에 따름)에 따라 보존될 수 있습니다.

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

11 정치 활동 및 기부금

외국 세력의 영향력, 선거 자금, 선물 및 접대, 입법·시민사회·친선·규제 관련 로비, 조달, ‘페이-투-플레이(pay-to-play)’, 증권 등과 관련된 다양한 법률이 Citi 및 그 공급업체의 정치 활동과 이러한 활동과 관련된 정보 공개를 규제하고 있습니다. 공급업체가 Citi의 관련 정책이나 기준, 법률 또는 규정을 준수하지 않는 모든 정치 활동은 금지됩니다.

정치 활동에는 다음 사항이 포함될 수 있지만, 이에 국한되지는 않습니다.

1. 기업 차원 또는 개인적 차원에서 정치 기부금을 제공하는 것, 정치 기부금을 모금하는 것, 공직이나 정당의 위원회 또는 정치적 위원회를 목표로 선거 운동하는 후보자를 위해 회사 자금이나 자원(시설, 장비, 소프트웨어 또는 직원과 같은)을 사용하거나 근무시간 중에 개인적인 서비스를 자원하는 것,
2. 직접적으로 또는 제 3자를 통하여 공직자에게 로비를 하거나 접촉을 시도하는 것. 여기에는 공직자, 입법에 영향을 주려는 시도가 포함되며, 관할 지역에 따라서는 정부기관의 규칙 제정 또는 정부 계약 수주에 영향을 미치려는 시도가 포함됨, 또는
3. 정부 부처, 위원회 또는 기타 유사한 조직을 포함하여 정부와 관련된 정치적인 자리를 구하거나, 수락하거나 보유하는 것.

어떤 정치적인 활동도 Citi의 글로벌 대정부 업무 글로벌 운영 부서의 사전 서면 승인 없이 공급업체가 Citi 또는 고객을 대리하여(또는 대리하는 것으로 알려지게) 맡거나 수행하여서는 안 됩니다. Citi는 로비활동 등 공급업체가 제공한 허용 가능하며 위탁된 정치활동 서비스를 위해 수수료를 지불하고/지불하거나 개인부담금을 상환할 수 있지만, 모든 종류의 개인 또는 기업 차원의 정치적 기부금을 공급업체나 공급업체 직원에게 환급하지 않습니다.

12 자금세탁방지(“AML”)

고객 관련 특정 서비스(예: 온보딩, 고객 계정 및 거래 심사)를 수행하거나 앞서 언급한 활동과 관련된 데이터/지표를 제공하는 공급업체 및/또는 금융 거래 또는 금융상품과 관련하여 중개자 역할을 수행하는 공급업체(예: 원격 수표 입금, 택배, 현금 수송차 또는 랍박스 서비스, 전자 송금, 디지털 자산)에 적용됩니다.

12.1 AML 의무:

1. Citi 프로세스 및 관련 법률 준수:

- (i) 그램-리치-블라일리법 및 그에 따라 공포된 규정, (ii) 미국 애국자법 및 그에 따라 공포된 규정, (iii) 자금세탁을 다루는 모든 법률 또는 규정, (iv) 경제 제재와 관련된 모든 법률 또는 규정을 포함하여 해당 법률의

요구 사항을 충족하도록 설계된 Citi 프로세스 및 절차를 유지하고 준수합니다. 이러한 정책과 절차는 금융 활동, 거래, 현금 유입과 관련하여 이상하거나 잠재적으로 이상해 보이는 활동을 신속히 보고해야 하는 요건을 포함하여 자금세탁방지 역할과 책임을 다룹니다.

2. 직원을 위한 연간 교육 및 프로그램 요소:

- 금융 활동, 거래, 현금 유입과 관련하여 이상하거나 잠재적으로 이상해 보이는 활동을 신속히 보고해야 하는 요건을 포함하여 Citi 에 서비스를 제공하는 직원이 자금세탁방지 역할 및 책임에 대한 연간 교육을 받도록 합니다. 교육에는 다음 내용이 포함되며, 이에 국한되지 않습니다.
 - a. 의심스러운 활동의 신고 및 보고.
 - b. 고객 식별 프로그램(CIP), 제재 및 이름 심사, 고객 실사(CDD), 강화된 실사(EDD), **실질 소유자(UBO)**의 식별 및 확인을 포함하는 ‘고객 알기’(KYC) 프로그램.
 - c. 모든 관련 금융상품 및 활동에 대한 거래 모니터링.
 - d. 법률 및 규제 변경 사항과 중요한 AML 프로그램 변경 사항에 대한 보고를 포함한 정기 보고/측정 항목.
 - e. 현장 방문을 포함한 AML 프로그램 효율성의 테스트 및 관리.

3. 계약 조항 준수:

- 공급업체가 시행해야 하는 프로그램을 정의하는 계약 조항을 준수합니다.

4. 의심되는 침해에 대한 신속한 보고:

- Citi 또는 Citi 고객과 관련된 현금 유입, 금융 활동 또는 거래와 관련하여 비정상적이거나 잠재적으로 비정상적으로 보이는 활동을 포함하여 법률 위반 의심 사항이 있는 경우 즉시 Citi 에 서면으로 보고합니다.

5. 탈세 방지 및 보고:

- 사업을 운영하는 국가의 모든 해당 세법 및 규정 준수
- 어떠한 상황에서도 공급업체는 고의로 불법 탈세를 하거나 다른 사람을 대신해 그러한 탈세를 지원해서는 안 됩니다. 여기에는 납기가 되어 지불해야 하는 세금의 납부를 회피하는 행위나 세무당국에 정보를 은폐하는 행위를 지원하는 활동도 포함될 수 있습니다.

- 따라서 공급업체는 합리적인 탈세 예방 절차를 채택하고 Citi 와 관련된 위반 또는 위반 혐의는 서면으로 즉시 Citi 에 보고해야 합니다.

12.2 공급업체 내부 정책 및 절차:

공급업체는 현존하는, 그리고 향후 효력을 발하는 모든 AML 법률과 규정을 준수하는 데 필요한 적절한 내부 정책과 절차를 유지해야 합니다.

13 기록 관리

Citi 정보의 액세스/처리/저장 서비스를 제공하는 공급업체에 적용됨

Citi 에서는 Citi 정보를 보관하는 모든 공급업체가 Business Activity Owner('BAO') 또는 Citi 의 주 비즈니스 담당자와 협력하여 (i) Citi 의 기록 관리 목적을 위해 정보를 기록 또는 일시적 기록 정보로 식별 및 분류하고, (ii) Citi 의 Master Record Catalogue('MRC')에 따라 기록을 분류하고, (iii) Citi 의 보존 요구 사항에 따라 정보를 보관하고, (iv) 정보 보관 요건이 없는 경우 정보 수명 주기가 끝나면 정보를 적절하게 폐기할 것을 요구합니다.

BAO 또는 Citi 의 주 비즈니스 담당자는 공급업체가 MRC 의 Citi 기록 코드에 따라 기록을 식별하고 분류했으며 인벤토리가 최소한 매년 업데이트되도록 공급업체와 협력해야 합니다. 공급업체는 BAO 가 지시하는 기록 관리 요건을 따라야 할 의무가 있습니다. 정보 보유 요건이 적용되지 않는 한 폐기 적격 기준을 충족하는 기록은 가능한 한 빨리 적절하게 폐기해야 하지만, 보관 요건을 충족한 후 최대 6 개월을 넘기지 않아야 합니다. 일시적인 정보는 정보 보유에 해당되지 않는 경우 마지막 사용 후 2 년 이내에 반드시 파기되어야 합니다. 개인 정보가 포함된 일시적 정보는 정보 보유 대상이 아닌 경우 수집 목적이 충족되면 삭제해야 합니다. 공급업체는 정보 보유 명령을 통보받은 경우 Citi 정보의 파기나 변경을 반드시 중단하여야 합니다. 명확하지 않은 것이 있다면, 공급업체는 Citi 의 주 비즈니스 담당자 또는 BAO 에게 연락하여 확인해야 합니다.

DRIM 은 분기별로 국가별 보존 일정에 나열된 보존 규칙을 검토하고 필요에 따라 업데이트하여 규정 및 내부 변경 사항을 준수합니다. 공급업체에 영향을 미치는 변경 사항이 있는 경우 BAO 는 공급업체에 알립니다. 공급업체는 그 영향을 평가하고, 관련 시스템, 프로세스 및 재고에 대한 변경 사항을 이행해야 합니다. 공급업체가 소유하고 관리하는 기록 유형의 경우 BAO 로부터 통지를 받은 날로부터 90 일 이내에 이행해야 합니다.

Citi 를 대리하여 문서를 유지·관리하는 공급업체는 BAO 가 요청한 시간 내에 법적 절차나 기타 절차와 관련이 있다고 간주되는 모든 정보를 보존("보유"), 수집하고 생성할 책임이 있습니다. 공급업체는 요청 시 적용되는 계약 조건에 따라 요구되는 Citi 정보를 반환해야

합니다. 공급업체는 기밀 여부와 관계없이(예: 기밀, 비기밀), Citi의 주 비즈니스 담당자 또는 BAO의 승인 없이 Citi 정보를 폐기해서는 안 되며, 이 승인에는 폐기 대상 정보에 대해 유효한 정보 보관 요건이 없다는 확인이 포함되어야 합니다. 기록 관리 및 보존 요건과 모든 기타 정보 취급 요건은 달리 명시적으로 합의되지 않는 한 계약의 종료 또는 만기 후에도 유효합니다.

공급업체는 보관하고 있는 Citi 정보의 관리 감독을 담당하는 모든 공급업체 직원 목록이 기록되어 있는 문서를 유지해야 하고, Citi의 주 비즈니스 담당자 또는 기록 관리 담당자(Records Management Officer)와 정기적으로 만나 연락 담당자 이름, 세부 절차, 역할 및 책임 그리고 Citi의 공급업체 기록 목록을 검토하고 업데이트해야 합니다.

14 기업 복원력/사업 연속성

Citi가 사용하는 서비스 또는 호스트 기술 인프라/애플리케이션을 제공하는 공급업체에 적용됩니다. Citi Business Activity Owner(BAO)는 이러한 요건의 적용 가능성과 COB 요건을 해당 공급업체에 알려야 할 책임이 있습니다.

14.1 복구 자원

공급업체의 재난 복구 계획에는 자사의 주 사업장이 사용 불가능하게 될 경우 Citi에 모든 제품과 서비스를 인도할 수 있는 대체 자원이 반드시 마련되어 있어야 합니다. 동일한 재해 사건이 주 사업장과 복구 장소 양쪽에 영향을 줄 수 있는 위협을 최소화하거나 제거하기 위하여 복구 장소는 주 사업장과 지리적으로 충분히 멀리 떨어진 위치에 있어야 합니다.

1. 복구 자원은 정보 시스템에 국한되지 않고 Citi에 제품과 서비스를 계속 인도하기 위하여 필요한 모든 자원을 포함하고 직원, 빌딩, 업무 장비, 데이터 센터, 데이터 및 음성 네트워크 및 운송 서비스 등을 포함할 수 있습니다.
2. 애플리케이션 공급업체는 높은 가용성(High Availability, HA) 구성을 보장하기 위해 Hot/Hot 유형의 아키텍처를 구현할 수 있습니다. 이 아키텍처는 최소한 두 개의 동일하게 구성된 시스템이 가동되어 고객/사용자가 사용할 수 있어야 합니다. 이 모델이 제공하는 가장 중요한 특징은 대체 환경이 기본(프로덕션) 데이터 센터와 동시에 실행된다는 것입니다.

14.2 복구 서비스 수준

Citi에 효과적일 수 있도록 공급업체의 사업 연속성은 정해진 서비스 수준을 충족해야 합니다. 최소한, 공급업체의 사업 연속성 계획에서 다음에 대한 특정 값을 정립해야 합니다.

1. 복구 시간 목표(RTO)
2. 복구 포인트 목표

3. 복구 자원/기술 역량
4. 복구 기간

14.3 재난 복구 계획

공급업체는 사업 지속에 필요한 재난 복구 계획을 유지·관리하여(Citi가 요청할 경우 현재 테스트 및 정기 테스트의 증빙 자료 제공해야 함) 특정 위치에서 또는 특정 개인의 노력을 통해 제품/서비스를 제공하거나 여기에 따른 기타 의무를 이행하는 공급업체의 능력이 중단되더라도 공급업체는 대체 작업장·인력을 활용하여 즉시 제품/서비스를 제공하고 의무를 이행할 수 있는 능력을 갖춰야 합니다. Citi와 공급업체 간에 체결된 각 작업 발주서 발효일로부터 10 일(월력 기준) 이내에 Citi에 제출해야 하며, 그 이후 각 작업 발주서가 효력을 유지하는 기간 내내 재난 복구 계획의 사본을 연 1 회 제출해야 합니다. 공급업체는 자사가 재난 복구 계획을 발동하는 상황에서 Citi가 공급업체로부터 제품/서비스를 계속 받는 데 필요한 안내나 기타 정보를 Citi에 제공해야 합니다. 공급업체는 재난 복구 계획에 최소한 다음 항목이 포함될 것임을 이에 진술하고, 보증하며, 약정합니다.

1. 기술 가용성(서비스 거부/DoS), 기본 작업 위치 가용성(접속 거부/DoA), 직원 가용성(하청업체 포함)을 포함한 중단 사태의 영향을 완화하기 위해 업무 재배치, 업무 이전 및/또는 원격 액세스를 포함하는 복구 절차 및 전략,
2. 공급업체가 자사의 제품/서비스 사업장에서 분리된 2 차 재난 복구 사이트의 유지·관리 계획, 제품/서비스 사업장에서 분리된 별도의 위치에 백업 미디어 저장, 중복(복제 작업용) 통신 회선 및 서버 사용(이에 국한되지 않음),
3. 정전, 시스템 장애, 자연 재해나 기타 예측할 수 없는 상황으로 인한 제품/서비스의 장기간 중단에 대응하는 데 필요한 상세하고 문서화된 계획을 포함하여 상호 합의한 기간 내에 작업 재개에 필요한 제품/서비스 운영, 애플리케이션 백업·복원 프로세스 및 절차 포함,
4. 모든 콘텐츠를 보호하는 데 필요한 절차,
5. 교체 장비(예: 컴퓨터 장비) 관련 절차 및 제 3 자 계약,
6. 모든 오프사이트 생산 시설 관련 절차, 그리고
7. 공급업체의 재난 복구 계획에는 다음 항목이 포함되어야 합니다.
 - a. 공급업체는 제품/서비스에 부정적인 영향을 미칠 수 있는 재해가 발생하는 경우 즉시 Citi에 통보해야 합니다.
 - b. 공급업체는 해당 통지를 받은 후 24 시간 이내에 Citi에 대체 처리 시설에서 제품/서비스를 계속 제공하기 위한 계획을 제공해야 합니다.
 - c. 제품/서비스는 필수 복구 시간 목표(RTO) 내에 완전히 작동해야 하며, 이는 해당 계약에 별도로 정의되어 있지 않은 경우 Citi에서 중요도 등급이 "Enterprise Critical" 또는 "HIGH"인 프로세스의 경우 4 시간 내, Citi에서 중요도 등급이 "MEDIUM"인 프로세스의

경우 24 시간 내, Citi 에서 중요도 등급이 "LOW"인 프로세스의 경우 72 시간 내입니다. 그리고

- d. 공급업체 시설의 일부가 작동할 수 없는 경우, 공급업체는 다른 기업 고객보다 불리한 조건으로 Citi 를 대우하여서는 안 됩니다.

14.4 호스팅 서비스에 적용되는 재난 복구 계획 요건

공급업체가 Citi 에 호스팅 서비스를 관리하고 제공하는 경우, 다음 조항도 적용됩니다. 재난 복구 계획에는 최소한 다음 사항이 포함됩니다.

1. 정전, 시스템 장애, 자연 재해나 기타 예측할 수 없는 상황으로 인한 호스팅 서비스의 장기간 중단에 대응하는 데 필요한 상세하고 문서화된 계획을 포함하여 상호 합의한 기간 내에 작업 재개에 필요한 서비스 운영, 애플리케이션 백업·복원 프로세스 및 절차 포함,
2. 또한, 공급업체의 재난 복구 계획에는 다음 항목이 포함되어야 합니다.
(a) 공급업체는 서비스에 부정적인 영향을 미칠 수 있는 재해 발생 시, 이 상황을 2 시간 이내에 Citi 에 서면으로 통지, (b) 해당 재난 발생 통지 후, 24 시간 이내에 대체 업무처리 시설에서 호스팅 서비스를 계속 제공할 계획안을 Citi 에 제출, (c) 최초 통지 후 48 시간 이내에 호스팅 서비스 완전히 작동해야 함.
3. 공급업체는 요청 시 Citi 가 공급업체의 재난 복구 계획 및 사업 계획의 연속성과 함께 작동할 재난 복구 계획 및 사업 연속성 계획을 개발하는 데 필요한 정보를 공개하는 데 동의합니다. 그리고
4. 공급업체 시설의 일부가 작동할 수 없는 경우, 공급업체는 다른 기업 고객보다 불리한 조건으로 Citi 를 대우하여서는 안 됩니다.

14.5 재난 복구 계획의 변경

공급업체는 재해 복구 계획을 변경할 수 있지만, 해당 변경 사항으로 인해 서비스에 부정적인 영향을 미칠 가능성이 있는 방식(예: RTO 연장)으로 재해 복구 계획이 저하되지 않는 한 변경이 가능합니다. 공급업체는 변경한 재해 복구 계획의 모든 내용을 Citi 에 즉시 알리고 Citi 의 요청에 따라 Citi 가 변경 사항을 완전히 이해하고 대응할 수 있도록 변경 내용을 설명해야 합니다.

14.6 하청업체의 재난 복구 계획

공급업체는 공급업체의 모든 하청업체가 Citi 의 공급업체 요건에 부합하는 재난 복구 계획 및 관련 비즈니스 연속성 통제 수단을 유지·관리하도록 보장해야 합니다. 공급업체는 이러한 통제 수단 및 테스트 결과를 정기적으로 검토하는 것을 포함하여 하청업체를 적절히 감독하고, 확인된 모든 미비점이 적시에 시정되도록 보장해야 합니다.

14.7 재난 복구 계획 발동 및 위기 통지

공급업체는 다음 상황 발생 시, Citi의 주 비즈니스 담당자에게 즉시 통지해야 합니다.

1. 공급업체가 재난 복구 계획을 실행할 때,
2. Citi에 제공하는 서비스나 제품에 부정적인 영향을 미칠 상당한 가능성이 있는 공급업체나 그 하청업체와 관련한 심각한 문제, 위험, 경고 또는 사이버 사건 발생 시.

14.8 테스트

공급업체의 모든 복구 자원 및 계획은 생산 구현 후 120일(Citi에서 Enterprise Critical로 분류한 애플리케이션의 경우 90일) 이내에 테스트되어야 하며, 최소한 1년에 한 번(12개월마다) 테스트를 해야 합니다. 테스트는 Citi에게 인도되는 모든 제품 및 서비스에 대하여 복구 서비스 수준을 충족하는 공급업체의 능력을 보여주어야 합니다. 이러한 테스트는 포괄적이어야 하며 Citi에 제공되는 서비스의 전체 범위를 포함해야 합니다. 공급업체는 Citi에 공급하는 제품/서비스의 복구 테스트에 관하여 최소 30일 전에 Citi에 사전 통보를 제공해야 합니다. Citi는 복구 환경에서 애플리케이션의 비즈니스 기능을 검증하기 위해 Citi가 사용하는 애플리케이션의 공급업체의 복구 테스트에 참여하거나 이를 참관할 수 있습니다. Citi가 참여하기를 원하는 경우 공급업체는 테스트 수행 전 테스트 목표, 테스트 계획 및 테스트 사이트에 연결하는 데 필요한 절차를 Citi에 제공합니다. 각 테스트를 완료한 후 10일(영업일 기준) 이내에 공급업체는 테스트 목표, 테스트 계획 및 테스트 결과 요약서를 Citi에 제공합니다. 요약서에는 복구하는 데 필요한 기간과 테스트 결과의 증거(예: 스크린샷)를 포함해야 합니다.

14.9 불륨 검증

Citi가 Enterprise Critical로 분류한 애플리케이션을 호스팅하는 공급업체는 반드시 자사 COB / 재해 복구 환경에서 프로덕션 처리량을 처리할 수 있는 능력을 입증해야 합니다. Citi와 공급업체는 반드시 검증에 사용할 기법에 동의해야 합니다.

14.10 서비스 제공 과정에서의 Citi 시스템 사용

Citi나 Citi의 계열사가 요청할 때, Citi 시스템을 사용하는 공급업체는 Citi의 재난 복구 훈련에 Citi에 참여하며, 비용 환급이나 비용 청구 없이 참가해야 합니다.

14.11 테스트 결과 조치

공급업체의 테스트 결과가 목표 또는 해당 RTO를 충족하지 못하는 것으로 판명된 경우, 공급업체는 근본 원인 분석을 수행하고 확인된 결함을 즉시 해결해야 합니다. 이러한 조치를 시행한 후 공급업체는 초기 테스트 실패일(또는 관련 작업서에 명시된 기간)로부터 달력일을 기준으로 120일(Citi에서 Enterprise Critical로 분류한 애플리케이션의 경우 90일) 이내에 테스트를 다시 실행해야 합니다.

14.12 위기 관리

사업 연속성 계획과 관련하여 공급업체는 복구업무의 지휘 및 통제에 관한 위기관리 계획을 유지하여야 합니다. 최소한 공급업체의 위기관리 계획은 복구업무를 작동시키고,

위기 정보를 수집하고 배포하는 커뮤니케이션 및 상부 보고 프로토콜을 정의하고, 위기의 경우에 Citi와의 커뮤니케이션을 위한 통보 및 상부 보고 프로토콜을 포함시킬 수 있는 충분한 권한이 있는 특정 개인을 식별하여야 합니다.

14.13 사업 연속성 평가

공급업체는 Citi의 제 3자 사업 연속성 평가 프로세스를 따라야 합니다. 이는 사업 연속성 관련 Citi 요구 사항 및 법률 그리고/또는 규제 요건(Citi와 공급업체에 모두 적용될 수 있음)의 준수에 대한 공급업체의 정책, 과정, 통제를 평가하는 것입니다. 평가는 공급업체의 응답을 요구하는 설문지와 이를 뒷받침하는 증거로 구성되며 공급업체의 현장 방문을 포함할 수 있습니다. 평가 결과를 통해 문제나 우려 사항이 드러나거나 나타날 경우, Citi는 조사 결과를 문서화하고 공급업체와 협력하여 문제를 해결할 수 있는 방법을 찾습니다. 공급업체는 Citi의 우려 사항을 Citi가 합리적으로 만족할 수 있을 정도로 해결하기 위해 필요한 수정을 신속하게 하고/하거나 보완 통제를 추가해야 합니다.

14.14 운영 복원력

크리티컬 비즈니스 서비스는 제공이 중단될 경우 Citi, 고객 또는 금융 시스템에 상당한 부정적 영향을 미칠 수 있는 서비스를 말합니다. 공급업체는 Citi가 수시로 지정하는 크리티컬 비즈니스 서비스에 해당하거나 Citi의 크리티컬 비즈니스 서비스('크리티컬 비즈니스 서비스')를 지원하는 서비스 요소의 일체 중단이 Citi가 지정한 기간을 초과하거나, Citi가 공급업체에 수시로 통지할 수 있는 지정된 관련 지표('영향 허용 한도')를 위반해서는 안 됩니다. 영향 허용 한도는 서비스 제공이 중단될 수 있는 시간에 해당하는 명확한 시간 기준 지표로 표현됩니다. Citi와 공급업체는 지속적인 계약 거버넌스 프로세스의 일부로 영향 허용 한도를 매년 검토해야 합니다. Citi가 2개 이상의 규제 기관이 지정한 요건을 준수하기 위해 개별적으로 크리티컬한 비즈니스 서비스에 두 가지 영향 허용 한도를 지정해야 하는 경우, Citi는 해당 크리티컬 비즈니스 서비스에 별도의 영향 허용 한도를 지정할 수 있습니다. 공급업체는,

1. Citi가 설정한 해당 영향 허용 한도(들) 범위 내에서 서비스를 제공하지 못했다는 사실(또는 합리적으로 실패할 가능성이 높음)을 인지하는 즉시 실제 장애 및 그러한 장애가 미칠 영향의 완화 조치와 함께 Citi에 통지해야 하며,
2. 요청 시, 공급업체가 크리티컬한 비즈니스 서비스를 제공하는 데 필요한 인력, 프로세스, 기술, 시설, 정보를 식별할 수 있도록 Citi에 합리적인 수준의 지원을 제공해야 하고,
3. Citi가 다음을 수행할 수 있도록 Citi에 합리적인 지원을 제공해야 합니다.
 - a. 크리티컬 비즈니스 서비스나 공급업체의 운영에 심각하지만 납득할 만한 중단 사고가 발생한 경우, 각 크리티컬 비즈니스 서비스를 영향 허용 한도 내에서 유지할 공급업체의 능력에 대한 일체의 내부 시나리오 테스트 결과, 그리고
 - b. Citi가 취약점을 식별하고 공급업체의 능력을 향상하는 데 필요한 조치를 취할 수 있게 시나리오 테스트 이후에 배운 교훈에 대한

설명을 제공하여 미래의 혼란에 효과적으로 대응하고 복구하는 작업.

Citi의 내부 시나리오 테스트에서 Citi가 설정한 해당 영향 허용 한도(들) 내에서 서비스를 제공하는 공급업체의 능력에 취약성이나 한계가 식별되는 경우, 그리고 Citi가 지정한 그러한 영향 허용 한도(들) 범위 내에서 공급업체가 일체의 서비스를 제공하는 데 실패하는 사고가 발생한 후, 당사자들은 공급업체가 필요한 조치를 취할 계획(계획 실행 일정 포함)에 합의함으로써, 합리적으로 실행 가능한 범위에서 최대한 빨리, 그러한 취약성이나 한계를 해결하거나 완화하거나, 또는 영향 허용 한도(해당되는 경우)를 유지하지 못하는 원인을 근본적으로 해결해야 합니다.

14.15 에스크로 계약

Citi의 요청에 따라 공급업체는 (i) Citi 환경 내에서 운영될 소프트웨어를 Citi에 라이선스하거나 (ii) Citi에 호스팅 서비스를 제공하는 경우, 예치 자료를 Citi가 지정한 에스크로 대리인에게 예치하고 해당 에스크로 계약에 따라 예치 자료와 관련된 예치자 등록 일정표 또는 에스크로 대리인이 요구하는 기타 양식을 작성해야 합니다. 이후 해당 라이선스 또는 호스팅 서비스와 관련된 계약의 남은 기간 동안 공급업체는 업데이트된 버전의 예치 자료를 에스크로 대리인에게 예치하여 에스크로된 소스 코드와 기타 예치 자료가 Citi에서 사용하는 소프트웨어 또는 호스팅 서비스 버전에 적용되는 최신 소프트웨어 버전으로 최신 상태를 유지하도록 보장합니다. 소스 코드 또는 기타 예치 자료 업데이트는 Citi에 라이선스된 소프트웨어에 대한 업데이트 날짜 또는 Citi에서 사용 중인 호스팅 서비스에 대한 수정 날짜로부터 30일 이내에 에스크로 대리인에게 전달되어야 합니다. 공급업체는 에스크로 계약에 명시된 예치자의 모든 의무와 요구 사항을 완전히 준수해야 합니다. 공급업체는 설정 수수료, 연회비, 예치 수수료, 서비스 수수료 및 기타 에스크로 관련 수수료와 비용을 포함하되 이에 국한되지 않는 모든 에스크로 비용과 수수료를 전적으로 책임집니다. 공개 사유(Release Event)가 발생하는 경우 에스크로 대리인은 기본 계약 및 에스크로 계약의 조건에 따라 예치 자료를 Citi 또는 Citi가 지정한 자에게 전달해야 합니다.

소스 코드(또는 기타 예치 자료)가 Citi 또는 Citi가 지정한 자(공급업체가 직접 또는 해당 에스크로 계약에 따른 의무 이행을 위한 에스크로 대리인을 통해)에게 전달되는 경우, 소스 코드 및 예치 자료는 공급업체와 Citi 간의 관련 계약에 따라 기존 라이선스가 적용됩니다. 단, 각 라이선스는 Citi가 다음을 위해 합리적으로 필요한 대로 소스 코드와 기타 예치 자료를 사용하고 수정할 수 있는 권한을 부여하는 것으로 간주됩니다. (i) 소프트웨어 및 기타 예치 자료를 Citi의 시스템과 통합하고 호환성을 보장함, (ii) 소프트웨어 또는 기타 예치 자료가 해당 법률, 업계 표준 또는 시장 관행을 준수하도록 함, (iii) 소프트웨어 또는 기타 예치 자료가 기술 혁신에 맞춰 최신 상태를 유지할 수 있도록 함, (iv) 소프트웨어 및 기타 예치 자료가 기존 라이선스 범위 내에서 Citi 및 그 계열사의 비즈니스 목적을 충족할 수 있도록 함. 소스 코드를 사용하여 Citi 또는 Citi를 대신하여 개발한 수정 사항이 포함된 모든 소프트웨어 버전은 이 섹션의 모든 조항과 기본 계약의 적용을 받습니다. 단, 공급업체는 모든 수정 사항에 대한 권리, 소유권 또는 이익을 갖지 않으며, 모든 수정 사항에 대한 모든 지적 재산권은 Citi에 독점적으로

귀속됩니다.

공급업체는 소프트웨어에 사용된 제 3 자 소프트웨어의 소스 코드를 소스 코드 예치에 포함할 수 있도록, 그 소프트웨어를 제공한 제 3 자와 상업적으로 합당한 노력을 기울여야 합니다. 제 3 자가 공급업체에게 이러한 권리를 부여하지 않는 경우, 공급업체는 공개 사유 발생 후 해당 제 3 자 소프트웨어 라이선스 계약을 Citi 로 이전할 수 있도록 상업적으로 합당한 노력을 기울여야 합니다.

이 섹션에 따라 Citi 에 제공된 소스 코드는 해당 라이선스 소프트웨어 또는 호스팅 서비스에 대한 기존 라이선스의 적용을 받습니다. 단, Citi 는 소프트웨어가 기술 혁신에 맞춰 최신 상태를 유지하도록 하고 해당 법률을 준수할 수 있도록 비즈니스 및 운영 요구 사항과 관련하여 소스 코드와 소프트웨어를 사용하고 수정할 수 있습니다. 소스 코드를 사용하여 Citi 또는 Citi 를 대신하여 개발한 수정 사항이 포함된 모든 소프트웨어 버전은 해당 계약의 모든 조항을 따릅니다. 단, 공급업체는 모든 수정 사항에 대한 권리, 소유권 또는 이익을 갖지 않으며, 모든 수정 사항에 대한 모든 지적 재산권은 Citi 에 독점적으로 귀속됩니다.

15 글로벌 신원조회 기준

Citi 에 서비스를 제공하는 모든 제 3 자 공급업체에 적용됩니다.

15.1 개요 - 신원 조회

신원조회는 모든 해당 현지의 법률 및 규정에 따라 수행되어야 합니다. 본 문서 안에 기술된 모든 정보 및 자기 정보 공개는 공급업체의 대표자, 공급업체 직원, 하청업체가 적절히 제공해야 합니다. 이력서 상, 면접 중, 입사 양식상 또는 입사 과정 중 정보의 위조 또는 누락은 발견되는 시점과 관계 없이 현지법에 따라 Citi 의 업무 배정 거부 또는 종료의 근거를 성립할 수 있습니다. 수행한 조회에서 부정적인 결과는 발견되는 시점과 관계 없이 현지법에 따라 Citi 의 업무 배정 거부 또는 종료의 근거를 성립할 수 있습니다. 신원조회 완료에 대한 추가 정보는

https://www.citigroup.com/rcs/citigpa/storage/public/country_background_screening_requirements_tables.pdf 에서 확인할 수 있습니다.

15.2 기본 정보 수집 및 신원 검증

공급업체의 직원이 Citi 업무를 시작하기 전에 공급업체는 직원의 성명, 주소 및 (주소와 다른 경우) 본적, 전화번호 및 이메일 주소(해당되는 경우)를 수집하여야 합니다. 또한, 공급업체 직원은 신분을 입증하는 서류를 제공하여야 합니다. 이와 같은 서류에는 국가 ID 번호에 관한 정보 및/또는 서류, 사진이 있는 정부 발행 신분증 또는 여권 등이 포함됩니다.

15.3 제재 조사

Citi 데이터/시스템/네트워크 또는 Citi 사업장에 대한 액세스 여부와 관계없이, Citi 의 공급업체 요건

하청업체를 포함하여 Citi 를 대신하여 업무를 수행하는 모든 공급업체 인력 또는 Citi 공급업체의 지분을 25% 이상 보유한 소유자는 미국 재무부 해외자산통제국(OFAC)의 특별지정제재대상자 및 차단 대상자(SDN) 목록, 미국이 부과한 제재의 적용을 받는 지역 및 관할권 목록('미국 제재')뿐 아니라 유럽연합(EU) 통합 금융 제재 목록, 유엔(UN) 안전보장이사회 통합 목록, 영국(UK) 제재 목록 및 현지 관할권에 적용되는 법률과 규정에 따른 목록('비미국 제재')을 포함하여 미국 외 당국이 발행한 모든 제재 목록 및 제재 적용 대상 관할권 명칭에 대해서도 심사를 받아야 합니다.

OFAC 목록은 이 웹사이트에서 누구나 볼 수 있습니다.
<https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists>

15.4 이민법 준수

공급업체는 모든 직원이 배정된 국가에서 노동 허가를 받았음을 확인하기 위한 절차를 유지하고 이행하고 있음을 입증해야 합니다. 또한, 공급업체는 다음을 준수해야 합니다. (1) 모든 직원이 노동 허가를 받도록 하고, (2) 고용 자격 및 확인 요건을 포함한 모든 적용 법률, 규정, 정책을 준수하도록 합니다. 또한 공급업체는 직원이 모든 관련 이민법 및 규정을 준수하고, 수행하는 업무 및 활동에 적합한 범주의 체류 자격/비자를 소지하도록 보장하기 위한 절차를 입증하고 유지해야 합니다.

15.5 고용 이력

공급업체는 현지 규정에 따라 필요한 경우 지난 칠(7)년 또는 십(10)년에 대한 직원의 고용 이력을 검증해야 합니다. 개인의 고용 이력을 검증하여 고용주, 직위, 날짜 및 업무가 정확하게 표현되었는지 확인해야 합니다. 공급업체의 인력은 또한 Citi 또는 그 전신 회사(다음에 포함하되 이에 국한되지 않음: Citibank, Citicorp, Travelers, Salomon Brothers 및/또는 Smith Barney)에서 컨설턴트 또는 임시 근로자로 이전에 고용되거나 배정된 적이 있는 경우 이를 공개해야 합니다.

15.6 학력

공급업체는 직원의 최종 학력을 검증하여야 합니다. 정보 검증은 학교에 다닌 일자, 기관명, 주소, 취득 학위를 포함하여야 합니다.

15.7 범죄 경력

법이 허용하는 경우, 공급업체나 협력업체 직원은 본인이 범죄 행위로 체포, 검찰 소환, 법원 출두 명령, 공소, 기소, 또는 유죄 판결을 받으면 이를 Citi 에 공개해야 합니다. 여기에는 유죄 인정이나 이의 제기 포기 신청 및 재판 전 회피 신청이나 이와 유사한 프로그램에 참여하는 것을 포함합니다. 법적으로 허용되고 가능한 경우에는 범죄 기록 및/또는 지문 확인에 대한 행정적 검토를 업무 시작일 전에 완료해야 합니다. 법률에 의해 달리 금지되지 않는 한, 절도, 사기, 부정직, 신뢰 위반과 관련된 범죄 또는 현지 법률에 따라 다르게 정의된 유사한 범죄에 대한 형사유죄판결은 Citi 업무 배정 거부

및/또는 자격 상실을 초래할 수 있습니다. 다른 유죄판결은 해당 법규에 근거하여 업무 배정 거부 및/또는 자격 상실을 초래할 수 있습니다.

15.8 재심사

임무를 마친 공급업체의 직원에게 다시 Citi 업무를 배정하는 경우에는 재심사가 수행되어야 합니다. 재심사 요건에 대한 추가 정보는 https://www.citigroup.com/citi/suppliers/data/background_screening_requirements_tables.pdf를 참고하십시오.

15.9 해외 전근

모든 심사는 업무가 수행되는 국가의 규정에 따라 이루어져야 합니다. 공급업체의 직원이 새로운 국가로 이동하는 경우 해당 개인은 새로운 국가의 요구 사항에 따라 재심사를 받아야 합니다.

16 비용

계약상 상환 가능한 사업 비용을 청구할 자격이 있는 공급업체

16.1 개요

Citi는 Citi가 서면으로 사전 승인하고 공급업체가 Citi에 제품 및 서비스를 제공하는 것과 관련하여 발생한 합리적인 사업 관련 비용만 상환하며, 해당 계약 또는 Citi의 운영 비용 거버넌스 정책 및 관련 표준과 절차의 조건에 따라야 하고 Citi가 허용 가능한 것으로 간주되는 영수증, 송장, 여정표 또는 기타 형태의 문서를 통해 적절하게 입증되어야 합니다.

16.2 환급

이러한 비용들은 반드시 Citi의 청구서 작성 요건에 따라 적절하게 문서화한 형태로 Citi에 청구해야 합니다. 공급업체 비용은 Citi 직원이 공급업체를 대신하여 부담해서는 안 됩니다. 유효하고 승인된 비용 항목에 대한 환급을 위해 Citi에 제출된 모든 비용에는 (다른 모든 청구 요구 사항 외에도) 다음이 포함되어야 합니다.

1. 비용의 비즈니스 목적
2. 비용의 금액 및 설명
3. 비용의 장소 및 일자
4. 공급업체가 서비스를 제공하고 있는 프로젝트의 이름/설명
5. 해당 비용이 발생한 서비스를 요청한 Citi 담당자의 이름 및 업무 관계
6. 해당되는 경우 구매 주문 번호.

허용되는 환급 가능한 업무 비용에 대한 정보는 Citi 의 주 비즈니스 담당자에게 문의하십시오. 영수증, 청구서, 여행 일정 또는 Citi 가 수용 가능한 것으로 간주하는 기타 형식의 문서를 반드시 환급 청구서와 함께 제출해야 합니다. 환급금 청구서는 해당 계약의 조항 또는 해당하는 경우 Citi 의 운영 비용 거버넌스 정책 및 관련 기준 및 절차를 준수해야 하며, 해당 사업 스폰서 및/또는 주요 Citi 사업 담당자의 승인을 받아야 하고, 적절한 권한을 부여받고 해당 경비에 대한 충분한 금액을 관장하는 개인의 승인을 받아야 합니다. 이를 준수하지 않은 요청서는 상환되지 않습니다.

17 정보 보안(IS)

부록에 분류 및 정의된 Citi 정보에 액세스하거나 이를 처리, 저장 또는 관리하거나 Citi 브랜드의 인터넷 연결 애플리케이션을 호스팅하거나 Citi 네트워크 리소스에 연결되거나 Citi 시설에 동반자 없이 액세스해야 하는 하청업체를 포함한 공급업체에 적용.

17.1 개관

이 섹션에서는 Citi 에서 기대하는 정보 보호 제어와 관련하여 Citi 정보를 저장, 처리, 관리 또는 액세스하거나 Citi 애플리케이션을 호스팅하거나 Citi 네트워크에 연결되는 공급업체(공급업체 하위 프로세서 또는 하청업체 포함)에 대한 최소 요구 사항을 제공합니다. 이러한 요구 사항은 Citi 와 공급업체가 사업을 수행하는 지역에서 적용되는 법률 및 규제 요건과 가장 높은 산업 표준(예: ISO/IEC 27001/2)에 따라 정보가 보호되도록 보장합니다. 현지의 법률, 규정 또는 관련 업계 기준이 여기에 마련된 것보다 더 높은 기준을 세운 경우에는 공급업체는 반드시 그러한 법률, 규정 또는 기준을 준수하여야 합니다. 또한 공급업체는 다른 Citi 의 정책과 계약 조건에 대한 준수의 일부로서 추가적인 정보 보안 관행 및 절차를 구체화할 필요가 있을 수 있습니다. 만일 정보보안을 위해 추가적인 보안 관행이나 절차를 실행하기로 결정한 경우 공급업체는 반드시 그러한 실천 및 절차가 본 섹션에 정해진 최소한의 통제와 상충하지 않도록 해야 합니다.

17.2 정보보안 정책 및 거버넌스

공급업체는 정보보안 정책 및 기준을 반드시 문서화해야 합니다. 정책 거버넌스에는 역할과 책임이 명확하게 정의되어야 하며, 기술, 산업 표준, 법률 및 규제 요건의 현재 상태와 일치하도록 정책 및 표준의 연례 검토 및 업데이트가 포함되어야 합니다.

17.3 직무 분리

공급업체는 리스크를 경감할 수 있는 적절한 보완 통제가 존재하지 않는 한 Citi 정보에 접근권을 가진 어느 개인도 승인이나 탐지 없이 동일한 활동, 변경, 정보 시스템 또는 거래에 대한 지속적인 접속으로 두 가지 업무 기능이나 두 가지의 IT 기능 또는 두 가지의 통제된 정보 시스템 기능을 수행하지 못하도록 하는 절차를 반드시 갖추어야 합니다.

표 A

기능	기능 설명
개발 / 엔지니어링	소프트웨어, 하드웨어, 구성을 설계, 생성 또는 수정합니다. 예: - 새 애플리케이션 코드 및 관련 데이터베이스 스키마 설계 및 생성 - 인프라 제품 및 애플리케이션 구성 요소 엔지니어링 - 소프트웨어 및 서비스와 통합되도록 기술 제품 맞춤화
승인	구현할 코드 변경 사항의 프로모션을 승인합니다.
시스템 구현/관리	소프트웨어, 하드웨어 및 구성 변경 사항을 설치, 배포 또는 관리합니다. 예: - 프로덕션 인프라에 자동 또는 수동으로 코드 릴리스를 수행 - 기술 제품 또는 기기 설치 - 생산 데이터를 포함하는 시스템의 문제 해결 및 시정을 지원하기 위해 서비스 시작 또는 중지
권한 ID 활동 검토	변경 관리 활동 또는 보안 관련 시스템 이벤트(예: 감사 추적)를 확인
ID 관리	ID(사용자, FID, 봇), 권한 또는 비밀번호를 추가, 수정, 삭제
비즈니스 기능	기능 설명
비즈니스 거래 개시	비즈니스 거래를 개시(입력, 실행 또는 생성이라고도 함)하고 고객 정보를 변경
비즈니스 거래 승인	비즈니스 거래 승인(인가, 확인 또는 릴리스라고도 함)
IT 기능	기능 설명
네트워크 운영	네트워크 인프라 서비스를 제공하는 제품의 기기 관리 및 운영 지원. 지원합니다. 예: 네트워크 라우터, 스위치, 방화벽, 도메인 이름 서비스(DNS)
비-네트워크 운영	네트워크 인프라 서비스를 제공하지 않는 제품의 기기 관리 및 운영 지원. 예: 서버, 전화, 컴퓨터

17.4 정보 보안에 대한 경영진의 약속

Citi 브랜드의 인터넷 기반 애플리케이션을 호스팅하고/하거나 기밀 이상 등급으로 분류된 Citi 정보에 접속할 수 있는 공급업체는 Citi의 제 3자 정보 보안 평가(TPISA) 프로세스를 따라야 합니다. 이는 정보 보안분야에서 Citi 요구 사항 및 법률 그리고/또는 규제 요건(Citi와 공급업체에 모두 적용될 수 있음)의 준수에 대한 공급업체의 정책, 과정, 통제를 평가하는 것입니다.

평가는 공급업체로부터 설명을 뒷받침하는 증빙 자료를 첨부한 응답을 요구하는 보안 질문서로 구성되며 제 3자가 Citi의 기밀 또는 그 이상의 정보를 저장, 처리, 관리 또는 액세스하는 공급업체의 현장 방문이 포함될 수 있습니다. 또한, TPISA 제 3자 지속 모니터링 팀은 사이버 보안 모니터링 도구를 활용하여 공급업체를 모니터링할 수 있습니다. 이 도구들은 공개적으로 이용 가능한 정보를 활용하여, 인터넷에 노출된 시스템, 호스트, 애플리케이션 및 서버에 대해 지원 종료 소프트웨어, 악용된 오픈 포트, 보안 취약점 또는 기타 침해 징후 등의 사항을 식별합니다. TPISA 결과가 보안 결함을 식별하거나 지적하는 경우에는 Citi는 공급업체에 대한 통지에 결과를 문서화하고 그러한 문제를 시정하는 방법을 찾기 위해 공급업체와 협력합니다. 공급업체는 Citi의 우려 사항을 해결하기 위해 Citi의 단독 재량에 따라 필요한 수정 조치 또는 보안 통제를 신속하게 실시하고, Citi가 지정한 위험 등급에 따라 고위험 문제의 경우 180일, 중간 위험 문제의 경우 240일, 저위험 문제의 경우 다음 컴플라이언스 날짜 이전인 요구되는 기한을 준수해야 합니다.

1. 공급업체는 자체 정보 보안 표준, 정책 및 절차를 토대로 비즈니스 활동 및 관련 통제 수단을 정기적으로 평가해야 합니다. 정기적인 평가는 최소한 다음을 반드시 포함해야 합니다.
 - a) 공급업체가 IS 정책 및 기준의 준수를 보장하기 위해 공급업체가 사용하는 절차에 대한 평가
 - b) 공급업체가 사용하는 애플리케이션과 인프라, 공급업체의 협력업체(해당되는 경우)가 사용하는 IS 프로세스와 같은 지원 리소스에 대한 평가. 하도급업체는 공급업체의 비즈니스 활동을 지원하거나 이와 같은 평가를 수행하도록 Citi를 지원할 수 있습니다. 제 3자가 Citi에서 기밀 이상의 등급으로 분류한 Citi 정보를 접속, 처리, 관리, 폐기할 수 있는 협력업체와의 새로운 계약을 체결하거나 기존 계약을 갱신하는 경우에는 규정 준수가 요구됩니다.
2. 정보보안 리스크 평가(예: TPISA)의 결과로 드러난 문제는 반드시 문서화되어야 하며, 종결될 때까지 추적해야 하며, 해결책의 증거 자료를 Citi에 제출해야 합니다.
3. 만일 공급업체의 정보보안 관리 기능이 해외로 재배치되었다면, 공급업체는 이와 같은 재배치 전에 반드시 Citi의 문서화된 승인을 받아야 합니다.
4. 공급업체가 새 법인을 인수하는 경우 공급업체는 본 기준을 준수하기 위해 인수한 법인의 평가를 완료해야 합니다.
5. 공급업체는 Citi가 사전에 문서로 승인하는 경우를 제외하고는 보안 관리기능을 절대 외부에 위탁해서는 안 됩니다. 여기에는 Citi 정보의 저장, 처리 및/또는 전송하기 위하여 사용되는 시스템에 대한 방화벽 관리, 보안 환경설정 관리, 패치 관리 또는 정보보안 관리(ISA) 기능이 포함되며, 이에만 국한되지는 않습니다.

6. 공급업체가 Citi 정보를 포함하거나 Citi 브랜드인 소프트웨어 또는 웹사이트를 호스팅하는 경우, Citi 시스템 보안 테스트(SSTS) 표준에 따라 정기적인 취약성 평가를 수행해야 합니다. 그리고 평가 과정에서 발견되는 중대한 문제는 해당 표준에 명시된 기간 내에 시정되어야 합니다. SSTS 는 외부 배포에 승인되지 않았으므로 공급업체는 Citi Relationship Manager 와 협력하여 참조 문서를 준수해야 합니다. 또한, 공급업체는 관련 ISO/IEC 27001 정보 보안 관리 표준(또는 더 높은 표준 및 프로토콜을 설정하는 후속 정보 보안 관리 표준)을 준수하고 본 섹션(17)에 포함된 정보 보안 조항을 준수해야 합니다.
7. Citi 내부 네트워크상의 서버 및/또는 정보 시스템에 연결이 필요한 경우, 공급업체는 Citi 의 주 비즈니스 담당자에게 통지하여 현재의 연결 제공 프로세스를 따를 수 있도록 해야 합니다.
8. 공급업체는 Citi 정보의 무단 접속, 취득, 분실, 변형, 삭제에 대해, 또는 Citi 정보의 저장, 처리, 전송에 사용되는 정보 시스템에 대한 기타 위협에 대해 적절한 Citi 연락 담당자(Business Activity Owner, BAO)에게 신속하게 통지해야 합니다.
9. 공급업체는 모든 고위험 활동 또는 민감한 데이터의 변경 사항에 대해 해당 조치의 실행한 사람을 식별할 수 있도록 감사 기록을 확보해야 합니다.
10. 공급업체는 기밀 또는 그 이상 등급의 데이터가 스크린과 서류(예: 모니터링, 예외, 규제, 기타 보고서 포함)에서 반드시 숨김 처리되도록 해야 합니다.
11. 공급업체는 민감한 데이터의 인쇄, 기록, 또는 복사를 반드시 제한해야 합니다(자체 기기에 의한 것도 포함됨). 공급업체는 법률이나 규정에 의해 달리 금지되어 있지 않는 한 계약 기간 중 또는 계약 기간 종료 시에 합의된 시점에 모든 Citi 정보를 반환 또는 파기해야 합니다.
12. 공급업체는 Citi 정보에 액세스 권한을 지닌 모든 공급업체 관계자(직원, 계약자, 임시 직원, 협력업체 직원)이 비공개 또는 기밀 유지 계약에 서명하도록 해야 합니다.
13. 공급업체 직원에게는 반드시 직원 핸드북이나 유사한 문서를 제공해야 합니다. 이러한 핸드북이나 유사 문서에는 해당 공급업체의 행동 강령 및 인사부 규정 위반 시 진행될 징계 프로세스가 담겨 있어야 하며, 반드시 해당 직원이 그러한 내용을 인지하였음을 서약해야 합니다.
14. 공급업체는 직원 또는 직원이 아닌 사람이 해고되거나 사직할 때 모든 자산을 회수하는 프로세스를 갖춰야 합니다.
15. 기밀 정보가 보관되거나 어떤 방식으로든 웹사이트나 웹 접근이 가능한 시스템에 저장되는 경우 공급업체는 해당 정보를 Citi 에 공개해야 합니다. 이러한 공개 내용은 서비스 설명에 포함될 수 있습니다. 공급업체가 Citi 기밀 정보를 보관하거나 저장하는 경우, 공급업체는 본 계약 기간 동안 SSAE 18 감사(또는 Citi 가 승인한 권위 있는 후속 평가)를 연 1 회 수행해야 하며, 최소 연 1 회 이상 SSAE 18 감사 또는 Citi 가 승인한 권위 있는 후속 평가의 결과를 문서화하는 보고서 사본을 Citi 에 제출해야 합니다.
16. 공급업체가 합병·인수나 그와 유사한 거래에서 다른 법인을 인수하거나 다른 법인에 의해 인수되고, 그러한 거래가 서비스에 영향을 미칠 수 있으면 공급업체는 즉시 이 사실을 Citi 에 서면으로 통지해야 하며, 공급업체는 인수

또는 합병이 새로운 법인에 대한 정보 보안 평가를 수행하여 이러한 변화가 동일한 법인의 규정 준수에 영향을 미치지 않도록 보장해야 합니다.

17.5 하청업체 정보 보안 리스크

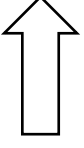
공급업체는 Citi 기밀 이상 등급의 데이터에 액세스 권한을 지닌 하청업체가 자격을 갖춘 정보 보안 인력이 수행하는 계약 전 및 계약 후 주기적인 정보 보안(IS) 평가를 받도록 요구해야 합니다. 이러한 평가는 시작부터 문제 관리까지 평가 프로세스의 모든 단계를 다루는 경영진이 승인한 프로세스에 따라 수행되어야 합니다. 하청업체에 대한 정보보안(IS) 평가 시, Citi의 제 3자 정보보안 평가 질문서(TPAQ)에 포함된 IS 영역과 일치하는 기준을 기반으로 하청업체의 보안 수준을 평가할 수 있는 질문서 또는 이에 상응하는 도구를 활용해야 합니다. 또한, 해당 하청업체와의 계약이 수반하는 IS 리스크를 논리적으로 산출할 수 있는 방법도 포함되어야 합니다. 공급업체는 평가 완료 상황을 추적하고, 지적된 문제 및 시정 조치 계획을 최종 해결까지 관리해야 합니다.

17.6 자산에 대한 책임

1. 공급업체는 Citi 정보를 저장, 처리 및/또는 전송하기 위하여 사용되는 자기 통제하에 있는 모든 어플리케이션 및 하드웨어의 목록을 유지하도록 하여야 합니다.
2. 공급업체는 Citi 정보자산의 목록을 자사의 통제 하에 유지관리해야 하며, 목록의 정확성과 온전성이 유지되도록 적절한 과정을 따라야 합니다.
3. 공급업체는 통제 하에 있는 모든 Citi 정보를 보호할 책임을 져야 합니다.
4. 공급업체는 업계 관행과 일치하는 방법으로 사용자의 활동에 대한 책임을 보장해야 합니다.
5. 외부 개인 인터넷 이메일 저장소 및 클라우드 저장소 계정의 사용자 접속은 Citi 정보가 있는 공급업체의 글로벌 네트워크로부터 제한되어야 합니다.

17.7 정보 분류 및 처리.

Citi는 아래의 정보 분류표에 따라 정보를 분류합니다. 아래 기재된 각 정보 분류의 정의와 예는 부록을 참고하십시오.

대외비(RESTRICTED)	최고 민감도
민감한 PII(SENSITIVE PII)	
기밀 PII(CONFIDENTIAL PII)	
기밀(CONFIDENTIAL)	
내부용 PII(INTERNAL PII)	
내부용(INTERNAL)	
공개(PUBLIC)	최저 민감도

1. Citi 정보 분류 등급을 토대로 Citi 는 공급업체와 협력하여 해당 정보를 보호하는데 필요한 보안 수준을 명시해야 하며, 공급업체는 Citi 가 요구할 수 있는 강화 또는 수정된 수준에 덧붙여 충분한 통제가 이루어지도록 해야 합니다.
2. Internal 등급 이상의 정보는 Citi 정책 및 기준에 부합하는 비밀보장 조항이 포함된, 제 3 자와 Citi 간 계약의 적용을 받는 제 3 자 관리 기기에 저장되어야 합니다.
3. 공급업체가 자사 소유가 아닌 기기를 사용하여 Citi 데이터(즉, 제 4 자가 관리하는 기기)를 저장하는 것을 허용하는 경우, 해당 공급업체는 이와 관련하여 별도의 경영진 승인을 의무화하는 정책을 마련하고, Citi 정보의 사용 및 폐기와 관련한 지침과 모니터링 절차를 확립해야 합니다.
4. 공급업체는 항상 Citi 정보를 무단 접근, 수정 또는 삭제로부터 보호하여야 합니다.
5. 기밀 등급 이상으로 분류된 Citi 정보는 전자전송매체(ETM)를 통해 전송되는 경우 승인된 암호화 알고리즘을 사용하여 암호화해야 하며, 전달이 확인되어야 합니다. 공급업체는 ETM 이 의도한 대로 수신되었는지 확인해야 합니다. 예상 배송일까지 수령 확인을 받지 못할 경우, 공급업체는 Citi 에 통보해야 합니다.

17.8 보안 구성

1. 공급업체는 Citi 정보를 저장, 처리, 액세스 또는 전송할 가능성이 있는 모든 자산에 대해 문서화된 보안 구성 표준을 유지 관리해야 합니다.
2. 공급업체는 정보보안 통제수단을 애플리케이션, 제품 및 서비스의 선정, 개발 및 실행에 관한 과정 및 절차에 통합하여야 합니다.
3. 공급업체는 Citi 정보가 저장, 처리 및/또는 전송되는 모든 시스템에 대한 보안 구축 절차를 갖추어야 합니다.
4. 공급업체는 모든 시스템에서 반드시 보안 이미지나 템플릿을 유지·관리해야 합니다.
5. 모든 기본 사용자 계정과 비밀번호는 공급업체가 지원하는 시스템, 네트워크 기기 및 애플리케이션에서 제거 및/또는 변경해야 합니다.

6. 손상된 시스템이나 서비스는 무결성이 검증된 이미지나 템플릿을 사용하여 다시 구축하고 구성해야 합니다.
7. 보안 구성에 실행할 모든 변경 사항은 공급업체의 변경 관리 프로세스를 통해 경영진의 승인을 받아야 합니다.
8. 공급업체는 보안 구성에 대한 변경 사항을 Citi 에 알려야 합니다.
9. 보안 구축 절차에는 프로덕션 배포 시점에 보안/기준 구축 세팅의 자동화된 환경 설정 확인을 지원하는 도구와 베이스라인 구성의 준수 여부와 편차를 지속적으로 모니터링하는 것이 반드시 포함되어야 합니다.

17.9 암호화 요건

공급업체는 암호화되지 않은 기밀 등급 이상의 정보를 전송해서는 안 됩니다. 기밀 등급 이상으로 분류된 정보는 Citi 가 승인한 도구 또는 솔루션을 사용하여 종단 간 암호화해야 합니다. 데이터의 암호화된 전송에 승인된 프로토콜 및 각 버전 번호는 다음과 같습니다.

1. 인증 및 권한 부여 정보를 교환할 때는 다음 요건을 준수해야 합니다. SAML v2.0, OAuth v2.0(인증 전용),
2. 통신 채널과 관련 키 교환을 보호하기 위해 다음과 같은 네트워크 보안 프로토콜만 허용됩니다.
 - a) TLS v1.3 이 선호되며 모든 TLS v1.3 제품군이 허용됩니다. TLS v1.3 이 유일하게 활성화된 프로토콜인 경우 추가 검토가 필요하지 않습니다.
 - b) TLS v1.3 이 기술적으로 사용할 수 없어 TLS 1.2 를 사용하는 경우, 현재 SSL Labs 에서 B 등급 이상을 받으면 허용되며 추가 검토는 필요하지 않습니다.

데이터가 Citi 제 3 자 환경에서 지속적으로 저장되거나 교환될 때는 반드시 Citi 가 승인한 도구나 솔루션을 사용해 완전히 암호화되어야 합니다. 데이터 암호화 시 승인된 알고리즘과 키의 길이는 다음과 같습니다.

1. **고급 암호화 표준(Advanced Encryption Standard, AES):** 승인된 키 길이: 256 비트 이상 제한 모드: ECB(Electronic Codebook) 모드는 일반 텍스트의 양이 블록 길이 이하인 경우를 제외하고 금지됩니다. 디스크 드라이브 암호화: 256 비트 키를 사용하는 AES 가 필요합니다. 128 비트 키 길이의 AES 는 TLS 암호화 방식 옵션으로 허용됩니다. 그러나 Citi 가 국제 일정을 준수할 수 있도록 2028 년 12 월 31 일부터는 256 비트 이상의 암호화 강도를 우선 적용하며, 128 비트 키 길이의 AES 는 허용되지 않습니다(참조: NIST 8547 IPD).
2. **ChaCha20(관련 사용 사례의 스트림 암호):** 승인된 키 길이: 128 비트 또는 256 비트, 96 비트 nonce 와 32 비트 블록 개수 또는 64 비트 nonce 와 64 비트 블록 개수. 최대 데이터 사이즈: 16 페타바이트.

승인된 공개 키 암호 시스템, 키 교환, 합의 메커니즘, 메시지 다이제스트 및 키 파생 함수는 다음과 같습니다.

공급업체의 양자 대비에 관한 통지: 공급업체는 NIST IR 8547(ipd)의 표 2 및 표 4 적용 범위에 대한 계획을 ([설문조사 링크](#))를 통해 Citi Quantum Readiness Program 팀에 제시해야 합니다.

1. 공개 키 암호 시스템 및 최소 키 길이 사이즈:

- a) Rivest-Shamir-Adleman(RSA): 2048 비트
- b) 디지털 서명 알고리즘(DSA): 2048 비트 Citi 외부에서 처리되거나 저장되는 Citi 데이터를 보호하는 데 DSA 를 사용해서는 안 됩니다.
- c) 타원 곡선 디지털 서명 알고리즘(ECDSA): 256 비트 및 NIST 권장 곡선을 사용하여 ANSI X9.62 에 명시된 대로.

2. 키 교환 및 합의 메커니즘 및 최소 키 길이 사이즈:

- a) Diffie-Hellman(DH) / Ephemeral Diffie-Hellman(DHE): 2048 비트
- b) Elliptic-curve Diffie-Hellman (ECDH) / Ephemeral Elliptic-curve Diffie-Hellman (ECDHE): 256 비트 및 NIST 권장 곡선을 사용하여 ANSI X9.63 에 명시된 대로¹.

3. 메시지 다이제스트 기능: 해시 생성에 사용된 자료의 임의 비트 수보다 긴 길이의 암호화 키를 생성해서는 안 됩니다.

- a) SHA-1 비디지털 서명 애플리케이션에만 사용할 수 있습니다. SHA-2 제품군, SHA-3 제품군 및 POLY-1305: 모든 암호화 해시 함수 애플리케이션에 사용할 수 있습니다.

4. 암호 기반 키 파생 함수 및 최소 요건:

- a) PBKDF2: 최소 10,000 회의 반복과 최소 16 바이트 이상의 솔트.
- b) HKDF: 반드시 솔트(Salt)를 추가하고 정보 입력 값이 포함되어야 합니다.
- c) SCRYPT: 최소 라운드 수/코스트 팩터는 10 입니다.
- d) 스트림 암호화에 NIST SP800-108 KDF 사용을 금지합니다. NIST SP 800-108 KDF 모드, 즉 카운터, 피드백 및 이중 파이프 라인 반복 모드가 허용됩니다.
- e) Argon2 를 추천합니다.

5. 비밀번호 해시 함수 및 최소 요건:

- a) Bcrypt(인증 자료 로컬 저장용): 최소 라운드 수/코스트 팩터는 10 입니다.
- b) 공급업체 제품이 배포된 환경이나 시스템에 비밀번호를 로컬로 저장하는 경우 비밀번호 해싱에는 Argon2 또는 PBKDF2 를 사용하는 것이 좋습니다.

17.10 외부 이메일

공급업체가 규정 및/또는 공급업체 정책에 따라 Citi 가 승인한 종단 간 암호화 소프트웨어 또는 도구를 사용할 수 없는 경우, Citi 정보 기밀 이상 등급의 Citi 정보가 포함된 개별 이메일에 대한 암호화 요건은 전송 암호화 기술(예: TLS(전송 계층 보안)를 통한

¹ ECDHE 가 선호됩니다.

게이트웨이 간 암호화)을 통해 완전히 충족할 수 있습니다. 승인된 보안 이메일 프로토콜은 다음과 같습니다.

1. **IBE(Identify-Based Encryption)**는 이메일 암호화 기능을 갖추고 있으며, Citi의 고객 대면 솔루션과 보안 이메일 및 eDelivery 시스템에 한하여 사용할 수 있습니다.
2. **MTLS(Mandatory TLS)**는 세션 암호화(이메일 페이로드를 암호화하지 않음)를 갖추고 있으며, 사전 협의를 통해 사용하기로 결정된 공급업체, 파트너 및 고객을 상대로 사용할 수 있습니다.
3. **DKIM(Domain Keys Identified Mail)**은 소스 인증 및 키 관리 기능을 갖추고 있으며, 공급업체·파트너·고객을 상대로 사용할 수 있습니다.

17.11 사설 네트워크

공인 기관에 의해 독립적으로 규제되며 면허 또는 인가를 받은 당사자 간 거래 업무(예: SWIFT 또는 중앙은행)를 위한 금융서비스 업계 기준을 충족하는 사설 네트워크는 해당 네트워크가 암호화된 전송을 완전히 지원하는 데 필요한 인프라를 제공할 때까지 기밀 PII 전송중 암호화 요건으로부터 면제되는 것으로 간주될 수 있습니다.

17.12 음성 및 팩스

팩스를 통하여 보내거나 음성 통화(인터넷 전화[VOIP] 포함)로 논의된 기밀 등급 이상으로 분류된 Citi 정보는 암호화되지 않고 전송될 수 있습니다. 필요한 경우 공급업체는 이러한 방법으로 전송되는 기밀 등급 이상의 정보를 보호하기 위한 구체적인 절차 및 지침을 개발해야 합니다.

17.13 암호 키 및 인증서 관리

이 섹션에서 사용하는 보안 경계라는 용어는 연방 정보 보호 표준(FIPS)과 같은 암호화 모듈 검증 프로그램(CMVP)의 검증 경계를 말합니다(FIPS 140-2/3 레벨 2가 최소 허용 보안 수준입니다). (AWS Nitro Enclave와 같은 기밀 컴퓨팅 인클레이브는 허용됩니다. 기타 고유한 보안 경계 케이스는 Citi에서 승인해야 합니다).

1. 공급업체는 암호화 및 서명(SSH 키 포함)에 최신 업계 표준 암호화 알고리즘과 최소 키 길이를 적용해야 합니다. 공급업체는 이러한 알고리즘과 키 길이가 업계 표준에 맞게 업데이트될 경우 변경 관리 프로세스를 통해 보증을 제공해야 합니다.
2. 공급업체는 민감한 자료의 무단 사용이나 노출을 방지하기 위한 통제 기능을 갖춘 공식적인 문서화된 키, 비밀 및 인증서 관리 수명 주기 프로세스를 갖추어야 합니다. 암호화된 모든 비밀과 키 수명 주기 이벤트는 보안 경계 내에서만 발생해야 합니다. 모든 특권 액세스 및 보안 경계에 대한 접근은 반드시 문서화되어야 합니다. 공급업체는 관련된 모든 주요 수명 주기 이벤트에 대한 시퀀스 다이어그램을 제공해야 하며, 관련된 행위자, 엔터티 및 경계를 강조해야 합니다.

3. 암호화된 키는 고유한 목적을 가져야 하며 디스크 암호화와 데이터 암호화에 동일한 암호화 키를 사용하거나 페이로드 암호화와 데이터베이스 암호화에 동일한 암호화 키를 사용하는 등 다른 목적으로 사용되어서는 안 됩니다. SaaS 공급업체가 여러 테넌트에 걸쳐 암호화 키를 재사용하는 것은 원칙적으로 금지되며, 명시적인 보안 아키텍처 위원회의 승인을 전제로 기밀 PII, 민감 PII 및 제한 등급 미만으로 분류된 Citi 정보와 관련된 비중요·저위험 사용 사례에 한해서만 허용될 수 있습니다.
4. 모든 암호화 키(대칭 또는 비대칭)의 경우 개인 키 또는 개인 키 자료(시드 또는 개인 키의 일부 등)는 어떤 경우에도 일반 텍스트로 표시되어서는 안 됩니다. 개인 키 또는 개인 키 자료(예: 시드 또는 개인 키의 일부)는 동적 세션 키와 같은 임시 키를 제외하고 보안 경계를 벗어나서는 안 됩니다. 설계에 보안 엔클레이브/특권 액세스 경계 간에 전송할 대칭 키나, 개인 키, 또는 개인 키 자료가 필요한 경우, 상호 TLS 암호화 터널을 통해서만 대칭 키 래핑 키 또는 공개 키 전송 키를 사용하여 암호화된 형태로 전송해야 하며, 이러한 전송은 Citi 에서 서면으로 승인을 받아야 합니다. 이 경우 개인 키 전송 키는 키가 생성된 특권 액세스 보안 경계를 벗어나서는 안 됩니다.
5. 대칭 키 래핑 키는 배포하기 전과 수동 키 입력/로드 시 두 개 이상의 키 구성 요소로 분할하고 XOR 처리해야 합니다. 대칭 키 래핑 키에는 CMVP 검증 모듈과 같은 보안 경계 내부에 연관된 적절한 액세스 제어 목록(ACL)이 있어야 하며 대칭 키 래핑 키는 보안 경계 외부에 저장되어서는 안 됩니다.
6. 개인 키 또는 비밀 또는 개인 키 자료(예: 시드 또는 개인 키의 일부)가 포함된 키 저장소 또는 보안 경계에 대한 사람 또는 서비스 또는 자동화된 에이전트의 액세스는 권한이 있는 직원 또는 시스템으로만 액세스를 제한하는 제어를 통해 적절히 분리되어야 합니다.
7. 개인 키나 대칭 키가 포함된 키 저장소에 대한 모든 액세스 요청은 감사 목적으로 액세스한 사람, 시기 및 목적과 같은 세부 정보와 함께 기록하고 문서화해야 합니다.
8. 공급업체는 자체 서명 인증서, 와일드카드 인증서 또는 기본 SSL 인증서를 사용해서는 안 됩니다.
9. 암호화된 모든 키에는 NIST SP800-57 파트 1, 개정 6 에 제안된 대로 암호화 기간이 정의되어 있어야 합니다. 변경 기간, 일정 충돌 및 시스템 정지를 감안할 수 있도록 키는 만료 전에 갱신 또는 교체되어야 합니다.
 - a) 만료된 인증서를 교체하는 동안 기존 비대칭 키 쌍을 재사용하는 것은 금지됩니다.
10. 암호화된 키는 키의 무결성, 키가 저장되거나 공유되는 매체 또는 대칭 키나 개인 키의 기밀성이 손상되는 것으로 의심되는 즉시 손상된 것으로 처리되어야 합니다. 손상된 키는 모두 운영에 사용할 수 없도록 제거해야 하며, 해당 인증서는 모두 취소해야 합니다.
11. 무선 네트워크는 업계 기준 암호화 알고리즘으로 암호화되어야 합니다.
12. 암호화 메커니즘 형태를 이용하는 공급업체는 업계 기준 키 관리 도구 및 기법을 사용하여야 합니다. 주요 관리 역할은 운영 관리와 분리되어야 합니다.

13. 공급업체는 Citi 데이터 보안 서비스가 제공하는 PKI 및 KMS 서비스와의 상호 운용성이 보장되고 암호화 통제가 Citi의 암호화 거버넌스 외부에 위임되지 않는 경우에만 클라우드 네이티브 KMS 및 PKI를 사용할 수 있습니다.

17.14 액세스 통제 책임

Citi 기밀 등급 이상의 정보를 저장, 액세스, 관리, 처리, 전송할 때 사용되는 모든 통제된 정보 시스템을 무단 액세스로부터 보호하기 위해, 공급업체는 각 직무에 필요한 최소한의 접근 수준으로 사용자 권한을 제한하고 모든 시스템과 애플리케이션에 대한 논리적 접근 제어를 관리하여 최소 권한 원칙을 시행할 책임이 있습니다. 통제는 완전히 문서화되고 감사될 수 있어야 합니다. 잠재적인 인적 오류로 인한 과도한 권한 부여 리스크를 경감하고 업계 기준에 부합하도록, 비밀번호 재설정 및 활성화를 포함한 액세스 프로비저닝 및 프로비저닝 해제는 가능한 경우 자동화된 프로세스를 통해 수행해야 합니다.

1. 공급업체는 자사 조직 내 모든 사용자의 액세스 권한에 대한 책임이 있습니다.
2. 공급업체는 오로지 업무를 수행하는 데 꼭 필요한 권한과 자격만 사용자에게 부여하는 액세스 통제 기능을 구현해야 합니다.
3. 공급업체는 무단 사용을 방지하기 위하여 모든 기본 설정(default) 접속 기능을 제거하거나, 비활성화하거나, 보호하도록 하는 절차를 실행해야 합니다.

17.15 사용자 액세스 관리

공급업체는 Citi의 기밀 등급 이상의 정보를 처리, 저장 및 / 또는 전송하는 시스템 및 애플리케이션의 논리적 액세스 프로비저닝을 관리해야 합니다. 다음 내용이 포함됩니다.

1. 승인된 인증 시스템의 식별 및 목록 관리.
2. Citi 데이터에 대한 모든 액세스는 관리자나 관리자가 지명한 담당자 및 시스템 소유자가 승인해야 한다는 요건. 공급업체는 Citi 데이터에 접근할 수 있는 모든 직원에게 필요에 따라서만 접근 권한을 부여할 책임이 있음.
3. 이해 상충이나 메이커 체커(maker-checker) 규칙 위반이 발생할 경우 개별 사용자에게 어떠한 권한/기능 조합도 제공될 수 없다는 요건.
4. 각 시스템에서 사용자에게 부여/취소된 액세스 권한을 감독하고 관리하는 모니터링 프로세스.
5. 액세스 요청은 다른 사용자의 권한을 미러링하거나 복제하는 방식에 의존해서는 안 됩니다. 권한 확산을 방지하고 최소 권한 원칙을 적용할 수 있도록, 요청 시 비즈니스 근거와 함께 명시적인 역할/권한을 지정해야 합니다.

17.16 사용자 ID 및 인증

모든 공급업체의 통제된 정보 시스템은 세션 또는 거래를 시작하기 전에 Citi 정보에 접근할 수 있는 플랫폼에 접속하는 사용자 또는 시스템의 신원을 인증해야 합니다.

1. 사용자는 사용자 ID에 의하여 고유하게 식별되거나 기술 플랫폼에 매핑되어야 합니다.
2. 사용자는 승인된 인증 방법을 사용하여 기술 플랫폼에 인증되어야 합니다. 공급업체는 현재 승인된 방법에 대해 주 비즈니스 담당자(BAO)에게 문의해야 합니다.
3. 공유된 인증 인프라(예: 싱글 사인온, 단축 사인온 및 기타 공유된 인증 서비스)는 Citi 인증 요건을 따라 사용되어야 합니다. 공급업체는 주 BAO에게 연락해 현재 승인된 방법을 알아봐야 합니다.
4. 정보 시스템에서 사용자를 인증하는 데 사용되는 신원 확인 데이터(IVD)는 전송 및 저장 시 암호화되어야 합니다. 암호화 요건은 섹션 17.9을 참조하십시오.
5. 공급업체 인력이 Citi 시스템에 액세스하는 데 사용하는 모든 계정은 고유한 Citi 할당 식별자(예: GEID)에 매핑되어야 합니다. 추적성, 직무 분리(SOD) 적용 및 감사 준비 상태를 보장하기 위해 사람 사용자의 일반/공유 사용자 ID는 금지됩니다.

17.17 권한이 부여된 액세스 ID 및 임시 권한이 부여된 액세스

공급업체는 모든 ID의 목록을 유지하고, 권한 있는 액세스 권한을 보유하거나 기밀 PII 이상으로 분류된 정보를 포함하는 전자 저장소(비즈니스 애플리케이션을 지원하는 데이터 세트 또는 데이터베이스)에 액세스할 수 있는 ID를 식별해야 합니다. 공급업체는 이러한 ID의 무단 사용을 방지하는 통제 수단을 구현해야 합니다. 직원이 특권 ID 또는 앞서 언급한 전자적 저장소에 대한 액세스가 필요한 경우, 다음과 같은 임시 액세스 관리 프로세스를 통해 액세스가 허용되어야 합니다.

1. 요청자가 사전에 승인된 허가 받은 사용자 명부 상에 있거나 사용 시점에 승인을 득한 상태일 것.
2. 접속 권한이 부여되기 전에 변경/문제 티켓에 문서화된 근거가 있을 것.
3. 접근을 통해 수행된 활동에 대한 독립적인 검토를 포함할 것.
4. 임시 액세스 부여 기간이 종료되면 해당 액세스의 취소/해제를 시작하는 절차를 포함합니다.
5. 프로덕션 및 실행 후 안정화 액세스(예: 주요 업그레이드 또는 고장/수리 해결 후)가 최대 7일(캘린더 기준)까지 연장되도록 허용하는 것.

17.18 사용자 액세스 권한 검토

1. 공급업체는 최소한 반기마다 Citi 정보를 저장, 처리, 관리 및/또는 전송하는데 사용되는 통제된 정보 시스템에 대한 불필요한 사용자 권한을 검토, 확인 및 삭제하는 데 필요한 프로세스를 문서화하여 구현해야 합니다.
2. 사용자는 사용자 본인의 자격 또는 사용자에게 검토 책임을 위임한 개인의 자격을 검토하거나 승인해서는 안 됩니다.
3. Citi 내 공급업체 직원이 담당 업무를 변경한 후 공급업체는 14 일(월력 기준) 내에 액세스 및 권한 검토를 수행하고 직원의 새로운 담당 업무에 기존 액세스가 더 이상 필요하지 않은 경우, Citi 데이터 액세스 권한을 제거해야 합니다.

17.19 안전한 로그인 절차

1. 잠겨진 사용자 로그인 ID 는 업계 기준 재설정 서비스 또는 다른 승인된 기능을 통하여 다시 활성화되어야 합니다. 운영 시스템 또는 애플리케이션이 지원하는 배너 텍스트는 사용자가 처음 등록하거나 인증을 받는 모든 네트워크의 시작 포인트에서 표시되어야 합니다.

17.20 비밀번호 관리 시스템

1. 사용자의 고정 비밀번호는 화면에 일반 텍스트로 표시되어서는 안 됩니다. 다음 조건을 충족하는 경우 비밀번호 표시 전환 기능은 이 요건에서 제외됩니다.
 - (1) 비밀번호 입력 시 기본적으로 가려집니다.
 - (2) 명시적인 사용자 작업을 통해서만 비밀번호 표시를 활성화할 수 있습니다.
 - (3) 사용자 작업이 중단된 후 최대 15 초 이내에 비밀번호가 자동으로 다시 가려집니다.
2. 특권 기능 ID 암호는 선명한 텍스트로 변경할 수 없게 기록되어서는 안 됩니다.
3. 고정 비밀번호는 최소 10 자 이상으로 구성되어야 하며, 문자와 숫자 모두를 포함해야 하고, 대소문자를 구별해야 합니다. 고정 비밀번호의 대소문자 구분은 각 인증 시점마다 검증해야 합니다. 2026 년 8 월 31 일 이후에 배포되는 애플리케이션에서 기능 ID(FID)의 고정 비밀번호는 최소 15 자 이상이어야 합니다.
4. PIN 은 실물 기기의 제약(예를 들면, 키패드, 전화, 스마트 카드)을 충족하기 위하여 필요한 경우에만 정보 시스템에 대한 접속을 인증하는 유일한 방법으로 사용될 수 있습니다.
5. 모든 고정 비밀번호는 최소 90 일마다 변경되어야 합니다.
6. 모든 고정 비밀번호는 로그인 시도가 연속 6 회 실패하거나 비밀번호 재설정 시도가 연속 6 회 이루어진 경우 잠겨야 합니다. 비밀번호는 ID 관리자 기능을 통해 잠금 해제되거나 최소 30 분 후에 자동으로 잠금 해제되어야 합니다.
7. 모든 인증 시스템은 100 일을 초과할 수 없도록 로그인 비활동/미사용 제어를 적용해야 합니다. 기술적으로 가능한 경우 비활성화된 로그인은 사용자나 다른 승인된 부서에 의해 다시 활성화될 수도 있습니다.

8. 인증 과정은 최근 사용한 6 개 비밀번호와 동일한 비밀번호가 사용되지 않도록 보장해야 합니다.

17.21 시스템 유틸리티 사용

공급업체는 시스템 및 애플리케이션 통제를 중단시킬 수 있는 유틸리티 프로그램의 사용(예: 주변기기로부터 부팅)을 제한하고 통제해야 합니다.

17.22 세션 시간 초과

1. 로그인 및 재인증은 Citi 정보를 저장, 처리 및/또는 전송하는데 사용되는 통제된 정보 시스템의 모든 사용자에게 반드시 발생해야 합니다.
2. 사용자는 30 분을 초과하지 않는 비활동 기간 후에 재인증해야 합니다. 활동은 엔드포인트(마우스, 키보드, 터치스크린 등)로의 일체의 입력을 포함합니다. 비밀번호로 보호된 스크린 세이버에서 실행이 되는 경우에는 애플리케이션 / 싱글 사인 온 실행은 필요치 않습니다.

17.23 사용자 액세스 종료

1. 데스크톱/Active Directory 의 사용자 로그인, SSO(Single Sign-on), 이메일, OTP(One Time Password) 토큰 및 원격 액세스를 포함한 Citi 기밀 등급 이상의 데이터에 대한 액세스를 허용할 권한을 지닌 담당 직원의 고용 종료나 사직 시에는 그러한 직원의 사용자 액세스나 권한을 다음 영업일 종료 전에 제거해야 합니다.
2. 직원이 Citi 가 소유 및 관리하는 시스템에 접근할 수 있는 경우 해당 직원의 직무 변경이나 고용 종료 시 Citi Business Relationship Manager, BAO, 또는 BAO 지원팀에 즉시 알려 Citi Business Manager 가 고용 종료된 직원의 종료 날짜가 끝나기 전에 접근 권한 제거를 개시하도록 해야 합니다.
3. 공급업체는 직원 또는 비직원이 고용 종료되거나 사임할 경우 섹션 17.23.2 에 명시된 기간 내에 모든 자산에 대한 접근 권한을 회수하기 위한 문서화된 프로세스를 갖추고 있습니다.
4. 공급업체가 17.23.1-17.23.3 과 관련하여 이상 사항을 발견한 경우, 공급업체는 타당한 근거와 통제 조항을 포함하여 Citi Business Relationship Manager(BAO) 또는 BAO 지원팀에 즉시 알려야 합니다.

17.24 원격 액세스

공급업체는 다음과 같은 Citi 기밀 등급 이상의 데이터를 저장, 처리 또는 전송할 수 있는 네트워크에 대한 액세스를 보호하는 데 필요한 원격 액세스 통제 기능을 갖춰야 합니다.

1. Citi 정보를 저장, 처리, 관리 및/또는 전송하는 데 사용되는 정보 시스템에 대한 원격 접속은 무단 사용으로부터 보호되어야 합니다.
2. Citi 정보의 저장, 처리 및/또는 전송에 사용되며 공급업체가 관리하는 모든 랩톱 및 공급업체가 관리하는 모든 데스크톱 기계, 그리고 Citi 정보 분류에서

기밀 등급 이상의 등급으로 분류된 Citi 정보를 로컬 저장/처리가 가능한 곳에서 원격 액세스를 이용하는 랩톱 및 데스크톱은 반드시 업계 기준을 충족하는 암호화 도구를 이용하여 암호화되어야 합니다.

3. 원격 연결은 다단계 인증(MFA)을 사용하는 승인된 원격 액세스 솔루션을 통해서만 설정해야 합니다.
4. 공급업체가 관리하는 기계가 인터넷에 직접 연결(즉, 공급업체가 관리하는 방화벽이나 프록시를 통하지 않고)된 경우 개인적인 방화벽을 갖추어야 합니다.
5. 공급업체가 관리하는 기기는 반드시 Citi 네트워크에 주기적으로 연결하여 소프트웨어 정기 업데이트, 소프트웨어/안티바이러스 도구 업데이트를 전송받고 설치해야 합니다. 해당 기기 업데이트의 목적으로 제한된 액세스가 허용될 수 있습니다.
6. 공급업체가 소유하지 않고 관리하지 않는 기기를 사용하여 Citi 기밀 등급 이상의 정보에 액세스하는 경우, 반드시 로컬 컴퓨터 다운로드를 허용하지 않는 승인된 솔루션을 사용하도록 구성해야 합니다. 다음의 통제 기능을 갖추어야 합니다.
 - a) Citi 데이터가 회사 관리 솔루션 외부 기기에 다운로드하는 것을 방지하는 통제 기능.
 - b) 해당 공급업체는 이와 같은 접속이 기준 원격접속기술(예: 가상 데스크톱 인터페이스(VDI))을 이용한 토큰에 기초하거나 인증서에 기초한 인증에 의해 안전하도록 보장해야 합니다.
 - c) 터미널 서비스 및 VMware Horizon 과 같은 원격 액세스 솔루션은 Blast, PCoIP 를 통한 클립보드 공유 및 드라이브 매핑을 비활성화하고 RDP 및 SSH 프로토콜을 비활성화하도록 구성해야 합니다.
7. 소프트 토큰이 MFA 에 사용되는 경우, 예를 들어 모바일 기기에서 소프트웨어 애플리케이션에 접근할 때, 해당 소프트 토큰 인증 소프트웨어는 사용자를 인증해야 하고(예: 암호, 생체 인식 등) 이른바 "탈옥"하거나 루팅한 휴대폰(모바일 기기 공급업체가 인증·제공한 운영 체제 이외의 운영 체제 사용 폰)의 경우 사용을 방지해야 합니다.
8. 정규/임시 직원, 계약업체 및 하청업체를 포함하되 이에 국한되지 않는 모든 공급업체의 직원은 다음을 포함하되 이에 국한되지 않는 시스템, 데이터 리포지토리, 애플리케이션 및/또는 인프라에 대한 특별, 권한 및/또는 관리 수준의 액세스가 필요합니다. 여기에는 시스템 관리자, 데이터베이스 관리자, 액세스 통제 관리자, 방화벽 관리자, 웹 사이트 관리자 등 Citi 에 제공되는 서비스와 직간접적으로 관련된 모든 사람이 포함됩니다(이에 국한되지 않음). 이러한 사람들은 MFA 을 통해서만 인증되어야 하며, 그러한 액세스는 이러한 요건에 명시된 의심스러운 활동 및/또는 무단 액세스 감시 의무를 충족하기 위해 공급업체에 의해 독립적으로 기록되고 모니터링되어야 합니다.
9. 개인 소유 기기와 제 3 자가 소유한 기기의 경우 공급업체는 해당 기기가 네트워크에 로그인하기 전에 해당 기기에 승인된 운영 체제 버전, 패치 수준, 바이러스 백신 및 맬웨어 방지 솔루션이 있는지 확인하는 효과적인 솔루션을 보유해야 합니다.
10. 공급업체는 모든 직원이 다음을 수행하도록 해야 합니다.

- a) 음성 지원 기기(예: Siri, Alexa), 비디오 녹음 기기 및/또는 기타 사진, 비디오 또는 오디오 청취/녹음 기기가 포함되지 않은 원격 작업 전용 공간을 유지·관리해야 합니다. 권한이 없는 사람이 원격 컴퓨팅 시스템의 화면에 표시될 수 있는 데이터, 시스템, 애플리케이션을 절대 볼 수 없게 하여야 합니다.
- b) 자리를 비울 때는 컴퓨팅 기기를 잠가 권한 없는 사람이 화면을 무단으로 볼 위험을 적절히 경감해야 합니다.

17.25 클리어 데스크 정책

공급업체의 직원은 그들의 근무장소에서 사용되거나 저장된 실물 정보를 포함하여 모든 형태의 Citi 정보를 보호해야 합니다. 공급업체는 정보 보안 교육이나 다른 채널을 통해 해당 요건을 모든 직원에게 적어도 연 1 회 알려야 합니다.

17.26 화재 안전

- 1. 공급업체는 물리적 보안과 현지 소방법을 포함한 안전한 근무 환경의 구축을 규율하는 해당 법적 및 규제상 요건을 준수해야 합니다.
- 2. 공급업체는 화재 감지, 경보 및 진압 시스템(들)을 이용하여야 합니다. 시스템은 반기마다 검사하고 매년 시험해야 합니다.

17.27 물리적 보안

- 1. Citi 정보는 오직 승인된 직원에게만 접근을 허용하는 통제를 갖춘 안전한 구역에 저장되어야 합니다.
- 2. 공급업체는 문서화되고 감사 가능한 물리적 접속 통제 시스템을 갖추어야 합니다.
- 3. 공급업체는 해당 환경 및 제공되는 서비스에 적절하게 제 3자가 모니터링하는 보안 경보, 보안 요원 및 비디오 감시를 포함하는 보안 경보와 침입 시스템의 조합을 활용해야 합니다.
- 4. 공급업체는 모든 방문자가 도착, 출입 시 검증 가능한 신분증을 제시하도록 요구하는 문서화된 방문자 정책을 갖추어야 합니다.

17.28 운영 관련 보안 절차 및 책임

- 1. 공급업체 변경 관리 프로세스에는 변경 등록, 검토, 테스트, 승인, 구현 및 종료를 중심으로 한 주요 체크포인트 통제가 포함되어야 합니다. 공급업체는 또한 의무적 승인 계층을 포함하여 모든 단계가 나열된 긴급 변경 프로세스를 갖추어야 합니다.
- 2. 공급업체는 가용성, 역량 및 성과 메트릭스/지표, 비즈니스 영향 평가, 성과 및 역량 문제의 사전 추적, 조사 및 해결을 포함하되 이에 국한되지 않는 역량 관리에 대한 감사 가능한 프로세스를 보유해야 합니다.

3. 해당되는 경우 공급업체는 랩, 개발, 테스트 및 프로덕션 환경은 모두 물리적으로 및/또는 논리적으로 서로 분리되도록 보장해야 합니다.

17.29 소프트웨어 개발 요건

Citi 에서만 사용되도록 개발된 소프트웨어를 제공하는 공급업체에 적용됩니다. 공급업체는 이러한 요건을 준수하거나, 동등한 품질의 동등한 접근 방식을 갖춘 문서화되고 승인된 소프트웨어 개발 수명 주기(SDLC) 프로세스를 입증해야 합니다.

17.30 착수 및 계획 수립

공급업체는 Citi 의 요건 및 계약상 의무에 부합하도록 솔루션의 범위와 목표를 정의해야 합니다. 다음 내용이 포함됩니다.

1. 기능 및 비기능 요구 사항 문서화
2. 소요 공수 및 일정 추정치 제공
3. 모든 제 3 자 구성 요소 또는 종속성 식별

보안 리스크 평가를 포함한 준수 활동은 프로젝트 착수 시 시작해야 합니다. 역할, 책임, 승인 점검 지점을 명확히 전달해야 합니다.

모든 환경은 개발(DEV), 테스트(TEST) 또는 운영(PROD)으로 분류해야 하며, 생애주기 전반에 걸쳐 엄격히 분리된 상태를 유지해야 합니다. 환경 분류에 따라 액세스 권한 및 처리할 수 있는 데이터 유형이 결정됩니다. 공급업체는 환경 지정에 따라 액세스를 제한하고, 무단 액세스 또는 데이터 노출을 방지하기 위해 적절한 SDLC 단계 완료 여부에 맞춰 배포를 조정해야 합니다.

17.31 설계

공급업체는 제공되는 솔루션이 명시된 모든 요건을 충족하도록 보장하는 설계 접근 방식('테스트 계획')을 문서화해야 합니다. 테스트 계획에는 최소한 다음 사항이 포함되고 설명되어야 합니다.

1. 1.요건 추적성을 갖춘 단위 테스트, 기능 및 비기능 테스트, 성능 측면 테스트를 포함하여 개발팀이 수행할 모든 테스트
2. 2.완료를 확인할 승인자 식별
3. 3.취약성 평가 및 위협 모델링과 같은 보안 테스트 요건
4. 4.테스트 환경, 접근 방식, 프로세스, 승격 경로

프로젝트 기간 동안의 릴리스 준비 기준, 내용 및 제공 주기를 포함하여 TEST 및 PROD 환경에 릴리스하기 위한 사전 요건과 프로세스를 명시하는 릴리스 전략을 마련해야 합니다.

계약에서 명시하는 경우, 소프트웨어 배포본은 Citi 가 승인한 도구 및 워크플로를 사용하여 Citi 가 승인한 형식으로 패키징해야 합니다.

17.32 테스트

테스트는 솔루션이 정의된 요건 및 성공 기준을 충족하는지 검증하기 위해 통제된 환경에서 계획하고 수행해야 합니다. 테스트 케이스는 요구 사항과 코드 커밋코드 커밋까지 추적할 수 있어야 합니다.

공급업체는 통과/실패 결과, 개발 중 수행한 추가 테스트 및 완료하지 못한 테스트(사유 포함)를 요약한 보고서(‘테스트 종료 보고서’)를 작성해야 합니다. 결함 및 연기된 기능은 미해결 문제에 대한 완화 계획과 함께 문서화해야 합니다.

Citi의 요청 시 공급업체는 다음의 증빙을 제공해야 합니다.

1. 자세한 테스트 계획
2. 테스트 종료 보고서에 상세히 기술된 테스트 완료 여부 및 결과
3. 테스트 결과를 요구 사항 및 코드 커밋까지 추적할 수 있는지 여부

17.33 배포

배포 전에 공급업체는 취약성 스캔 및 위협 모델링을 포함하여 필요한 모든 보안 테스트를 완료해야 합니다. 릴리스 프로세스는 문서화된 변경 기록, 롤백 전략, 필요한 승인을 포함하도록 구성해야 합니다. 구현 계획 및 배포 런북에는 모니터링 및 에스컬레이션 프로토콜을 포함해야 합니다.

배포 후 공급업체는 시스템 식별자를 확정하고 감사 준비 상태를 보장하기 위해 관련된 모든 산출물을 업데이트해야 합니다.

17.34 보안

1. 코드 작성 전에 잠재적인 보안 리스크, 취약성 및 아키텍처상 취약점을 식별하고 해결하기 위해 SDLC의 설계 단계에서 수행하는 체계적인 평가(‘보안 설계 검토’)를 OWASP 등의 업계 표준에 부합하는 예방 및 탐지 통제 수단과 함께 SDLC에 포함해야 합니다.
2. 반드시 보안 코딩 관행이 실행되도록 해야 합니다.
3. 공급업체는 정보보안 통제수단을 애플리케이션, 제품 및 서비스의 선정, 개발 및 실행에 관한 과정 및 절차에 통합하여야 합니다.
4. 공급업체는 Citi 정보가 저장, 처리 및/또는 전송되는 모든 시스템에 대해 안전한 빌드 절차를 마련하고, 모든 시스템에 대한 안전한 이미지 또는 템플릿을 유지해야 합니다.

17.35 악성 코드 통제

공급업체는 악성 코드(예를 들면, 바이러스, 웜, 트로이 목마 바이러스, 애드웨어, 스파이웨어, 랜섬웨어나 데이터 손상을 초래할 수 있는 기타 유사 사이버 공격)의 유입을 방지하고 탐지하기 위한 통제 수단을 구현해야 합니다. 공급업체는 반드시

1. 모든 개인용 컴퓨터에 안티바이러스 및 안티스파이웨어 기술을 실행, 업데이트 및 유지관리해야 하며, Citi 데이터를 저장, 처리 및/또는 전달하는 모든 근거리 통신망(LAN) 서버, 메일 서버 및 기타 기기에 기술을 실행, 업데이트 및 유지관리해야 합니다.
2. 최종 사용자가 안티바이러스/안티 맬웨어 도구 및 예약 검사를 비활성화하지 못하도록 보안 설정을 배포합니다.
3. 안티바이러스·안티 맬웨어 소프트웨어의 환경 설정 및 업데이트에 필요한 중앙 관리형, 자동화 절차를 갖춰야 합니다.

4. 안티바이러스 서명 또는 스캔 엔진이 낙후된 규정 준수 위반 컴퓨터를 식별하고 그에 대처하는 데 필요한 프로세스가 구현되었는지 확인합니다.
5. 저장 매체를 포함하되 이에 국한되지 않는 외부 기기에 대한 연결을 허용하는 통신 포트/인터페이스에 대한 액세스를 제어합니다.

17.36 모바일 코드 통제

공급업체는 안전한 모바일 코드 관행에 대한 통제가 구현되도록 해야 합니다. 공급업체는 모바일 코드의 사용이 승인된 경우에는 환경설정은 최소한 업계의 모든 관련 기준 및 Citi에 대한 계약상의 의무를 충족하고, 승인된 모바일 코드가 명백히 정의되고 문서화된 보안 정책에 따라 운영되고 무단 모바일 코드가 실행되는 것을 방지하도록 해야 합니다.

기초 운영 체제 또는 플랫폼(즉, “샌드박스(sandbox)” 외부)에 영향을 줄 수 있는 모바일 코드에 대해 공급업체는 다음을 확실히 하여야 합니다.

1. 공급업체가 발행한 모바일 코드는 Citi에서 승인한 인증 기관에서 서명해야 하며, 인증서의 수명 주기는 공급업체가 관리하여 인증서 만료 또는 교체를 처리해야 합니다.
2. 인증이 만료된 서명된 모바일 코드는 프로덕션에서 제거되어야 합니다.

17.37 감사 기록

공급업체는 Citi 데이터에 액세스하거나 Citi 데이터를 저장, 처리, 관리 및/또는 전송하는 데 사용되는 모든 통제된 정보 시스템이 다음 항목을 기록하기 위해 인프라 또는 애플리케이션 레벨에서 감사 추적 기능을 유지하도록 해야 합니다.

1. 연관된 플랫폼에 대한 인프라 보안 관련 활동
2. 방화벽 또는 IDS/IPS 생성 보안 이벤트와 관련된 모든 시스템 경보
3. 모든 시도된 시스템 보안 위반(예: 사용자 로그인 시도 실패)
4. 리소스(소프트웨어, 데이터, 프로세스 등)에 대한 무단 액세스 시도
5. 관리자가 취한 조치
6. 특정 사용자나 다른 시스템으로부터 특정 정보 수신 관련 정보
7. 특별히 다음 사항을 포함한 금융 거래 및 Citi 정보와 관련된 모든 중요한 이벤트:
 - a. 금융 거래 업데이트
 - b. 기밀 또는 민감한 PII 데이터 업데이트
 - c. 대외비 데이터 업데이트
 - d. 인증 데이터 업데이트
8. 연결되었던 모든 세션
9. 사기 수사의 지원을 위해 기술적으로 가능한 경우 Citi용 애플리케이션(즉, 웹사이트 및 모바일 애플리케이션)과 관련하여 고유 기기 ID와 같은 세션 아티팩트를 수집하고 기록해야 합니다. 이러한 아티팩트에는 최소한 IP 주소가 포함되어야 합니다. 이러한 아티팩트는 Citi 거래와 Citi 계정 개설

활동에 대하여 수집되어야 합니다. 세션 아티팩트가 거래 또는 계정 개설과 연결될 수 있도록 정보를 수집해야 합니다.

10. 감사 추적은 특정 활동이 특정 개인에 의해 수행되었음을 명확히 문서화하여 부인 방지를 보장해야 합니다.

11. 중요한 정보보안관리(ISA) 사건은 다음 사항을 포함하여 구체적으로 기록되어야 합니다.

- a) 사용자 생성
- b) 사용자 액세스 권한 수정
- c) 통제된 정보 시스템상의 프로파일 삭제, 생성 및 수정
- d) 비밀번호 재설정
- e) 시스템 보안 환경설정에 대한 변경
- f) 특권 기능 ID 의 모든 상호 활동
- g) 보안 기록은 기술적으로 불가능하지 않다면 기록을 생성하는 시스템에 상관 없이 최소한 다음 정보를 포함해야 합니다.
 - I. 사건의 일자 및 시간(UTC 형식의 시간)
 - II. 작업을 수행하는 개인의 사용자 ID
 - III. 이벤트 유형
 - IV. 영향을 받는 자산 또는 리소스 이름
 - V. 접근 유형(삭제, 수정 등)
 - VI. 이벤트 성공 또는 실패 여부
 - VII. 소스(단말기, 포트, 위치, IP, 호스트 이름 등)

17.38 로그(Log) 정보의 보호

공급업체는 감사 추적의 무결성을 유지하기 위해 시작, 종료, 보관, 전송 중에 액세스 통제를 구현해야 합니다.

- 1. 공급업체는 감사 기록의 무단 수정을 방지하기 위하여 감사 기록이 추적하는 시스템 사용자의 활동을 해당 시스템 사용자가 덮어쓰거나 수정할 수 없게 하는 통제 기능을 마련해야 합니다.
- 2. 공급업체는 로그 데이터의 유지 방법을 정의하고, 적용되는 모든 법적 및 규제 요건을 참조하는 준수 조치를 포함한 로그 데이터 기록 보존 절차를 Citi 에 제공해야 합니다.
- 3. 한 조직이나 보안 도메인 내의 모든 관련 정보 처리 시스템의 시계는 정확한 시간 소스와 동기화되어야 합니다.

17.39 시스템 사용 모니터링

공급업체는 다음 사건이 직접적으로 또는 자동화된 검토 과정을 통하여 파악, 기록 및 검토되도록 해야 합니다.

1. 방화벽 또는 침입 탐지 시스템(IDS)/침입 방지 시스템(IPS) 생성 보안 이벤트와 관련된 모든 시스템 경보
2. 안전한 기준 구조에서 확인된 중요한 자원에 대한 모든 업데이트
3. 기밀 PII 이상으로 분류된 정보에 액세스할 수 있는 모든 ID(기능, 특권, 시스템, 임시 등)에서 수행하는 모든 인터랙티브 활동
4. 위의 감사 기록(Audit Logging) 섹션에 나열된 중요한 ISA 사건. 단, 다음과 같은 예외 적용 사례가 있음:
 - a) 정보보안 관리 활동이 엔드 투 엔드 무결성 제어를 갖춘 자동화된 작업흐름/수행 시스템에 의하여 실행되는 경우 사용자, 역할 또는 프로필의 권한 제거.

17.40 기록 상관관계 및 검토

1. 기록된 사건으로 인해 경보가 발생하면 해당 사건을 검토해야 하며, 공급업체는 후속 조치를 시작하고 잠재적으로 유해한 정보 보안 사고가 발생했을 가능성이 있는 경우 조사를 진행해야 합니다.
2. 공급업체는 보안 정보 및 이벤트 관리(SIEM, Security Information and Event Management) 시스템 또는 로그 상관관계 분석과 검토에 필요한 로그 분석 도구와 같은 일원화된 중앙 로그 관리 시스템에 집계되도록 구현해야 합니다.
3. 공급업체는 조치가 필요한 이벤트 식별 능력을 개선하기 위해 SIEM 또는 로그 분석 도구의 구성 환경을 주기적으로 검토하고 조정해야 합니다.

17.41 운영 소프트웨어 통제

공급업체는 현재 업계에서 인정하는 상용 공급업체가 지원하는 운영 체제 및 소프트웨어만 활용하거나 보안 문제를 해결하기 위해 패치 및 구성 업데이트를 적극적이고 적절하게 릴리스해야 합니다.

공급업체는 승인된 모든 보안 패치 및 구성을 적용해야 하는 시정 기한을 명시하는 문서화된 프로세스가 구현되도록 보장해야 합니다.

공급업체는 자사와 Citi 간의 별도의 유지·관리 약정과는 상관없이 Citi를 위해 개발되고 라이선스 약정에 의해 규율되는 소프트웨어가 알려진 취약성이 있는 지원되지 않는 소프트웨어 버전의 사용을 허용하지 않도록 반드시 보장해야 하며, 해당 소프트웨어를 적시에 업데이트하고 패치 버전을 설치하여야 합니다.

Citi 정보를 처리하는 데 사용되는 애플리케이션 소프트웨어는 기존 공급업체로부터 조달해야 하며 라이선스를 받고, 카탈로그화하고, 지원 서비스를 받아야 합니다.

17.42 취약성 및 위협 관리

1. 공급업체는 다음을 모두 포괄적으로 다루고(다루거나) 포함하는 취약성 관리 프로세스와 위협 관리 프로세스를 구현해야 합니다.

- a. Citi 기밀 데이터 또는 보다 민감한 데이터를 처리, 저장, 액세스 또는 전송하는 데 사용될 수 있는 모든 자산의 취약점을 발견하고 관리하기 위한 도구 및 절차.
- b. 업계에서 인정하는 취약성 점검 도구 및 보고 방법론을 사용하여 최소 매주 스캔을 수행해야 한다는 요건.
- c. 최신 버전의 '공통 취약성 점수 시스템(CVSS)'에 따라 취약성을 순위를 매기고(<https://www.first.org/cvss> 참조), 심각도를 바탕으로 수정 일정을 정함.
- d. 전체 프로덕션 배포 전에 취약점 수정 테스트를 해야 한다는 요건.
- e. 중요한 취약점의 수정을 가속화하기 위한 문서화되고 반복 가능한 운영 프로세스.
- f. 공급업체는 자산의 지원 가능 수명 주기 전반에 걸쳐 자산을 추적하여 수명 종료(EOL) 또는 공급업체 지원 종료(EOVS) 상태에 대비하고, 그러한 자산을 사전에 업그레이드하거나 교체하기 위한 프로세스를 마련해야 합니다.
- g. 정보 수집, 취약성 스캔 또는 침투 테스트를 통해 식별된 CVSS 점수가 심각한 모든 취약성은 우선적으로 처리하고, 취약성 리스크에 상응하는 명확히 정의된 기한 내에 시정해야 합니다.

17.43 제 3 자가 호스팅하는 애플리케이션

공급업체가 웹사이트나 인터넷에서 액세스 가능한 시스템 또는 Citi 브랜드 웹사이트에 Citi 기밀 등급 이상의 민감 데이터를 유지하거나 저장하는 경우, Citi에 영향을 미치는 제품이나 서비스(각각 "취약성") 관련 취약성이나 위협으로부터 보호하는 차원에서 공급업체는 다음 요건을 준수해야 합니다.

1. 공급업체 직원 한 명을 Citi의 정보 보안 관련 문의 담당자로 지정해야 합니다.
2. 업계에서 인정하는 모범 사례를 활용하여 최소 주 단위로 모니터링하고, FIRST, CERT/CC, CISA 알려진 악용 취약점 카탈로그 및 벤더 메일링 리스트와 같은 평판이 좋은 컴퓨터 보안 취약점 정보 출처를 활용하며, Citi 관련 서비스를 획득, 철저히 테스트, 적용 및 제공하는 데 필요한 적절한 조치를 취하기 위해 상업적으로 합당한 노력을 기울이고 Citi에 서비스 팩, 패치, 업그레이드 및 우회 해결책을 제공해야 합니다.
3. 네트워크, 시스템, 애플리케이션 취약성 스캐닝 도구 및/또는 침투 테스트를 활용하여 정보 보안 조치 구현 상황을 최소한 분기별로 테스트해야 합니다.
4. Citi 또는 Citi가 승인한 제 3자가 합리적인 시간 간격으로 취약성 평가, 윤리적 해킹 또는 기타 보안 평가를 수행하여 공급업체가 계약 및 이러한 요구 사항에 따른 의무를 준수하는지 확인할 수 있도록 허용합니다. 여기에는 정책, 프로세스 및 절차 검토, 물리적 보안 조치에 대한 현장 평가, 네트워크, 시스템 및 애플리케이션 취약성 스캐닝, 상업적으로 이용 가능한 도구 및/또는 업계 표준 관행을 사용한 침투 테스트가 포함되지만 이에 국한되지 않습니다.

5. 공급업체에 취약성 평가 서비스를 제공하는 모든 계약자는 Citi 가 승인한 취약성 평가 제공자 목록에 속해야 합니다. 공급업체가 서비스를 제공하는 과정에서 계약업체나 하청업체를 이용하는 경우, 공급업체는 자신의 비용으로 요구되는 모든 취약성 평가가 공급업체가 해당 서비스를 직접 제공하는 것처럼 시기적절한 방식으로 완수되도록 보장해야 하며, 일체의 계약업체나 하청업체가 그러한 평가를 용이하게 수행할 수 있게 하여야 한다는 의무 조항을 공급업체와 계약업체/하청업체 간의 계약서에 명시해야 합니다. 이러한 의무 요건에는 Citi 가 그러한 평가 작업을 실시할 권한을 명시하는 조항도 포함해야 합니다.

6. **통지.**

a) 공급업체가 Citi 에 영향을 미치는 제품이나 서비스 관련 취약점을 식별하는 경우, 공급업체는 해당 취약성 식별 후 24 시간 이내에 서면으로 Citi 에 통지하고 공급업체가 취할 교정 조치에 대한 설명을 포함해야 합니다.

b) 공급업체가 프로세스 채널의 '책임 공개'(NVD, National Vulnerability Database)의 취약성 공개 또는 외부 보안 벤더에 제공하는 위협 카탈로그를 통한 공시) 이후의 시점에 Citi 에 영향을 미치는 제품이나 서비스와 관련된 취약점을 인지하게 된 경우, 그러한 공시가 이뤄진 시점으로부터 24시간 이내에 이러한 사실을 Citi 에 서면으로 통지해야 합니다. 각 통지에는 취약점에 대한 정보, Citi 관련 서비스에 대한 시스템의 유틸리티(즉, Citi 정보를 호스팅하는지 또는 서비스 제공에 사용되는지 여부), 원격으로 악용할 수 있는지 여부, 그리고 CVE(Common Vulnerabilities and Exposures) 점수에 대한 정보가 포함됩니다. 공급업체는 해당 취약점이 수정될 때까지 계속해서 Citi 에 업데이트 정보를 제공해야 합니다. Citi 가 취약성을 식별한 경우에는 Citi 측이 공급업체에 동일한 형태로 통지할 수 있으며, 공급업체는 이 섹션에 따라 취약점을 신속하게 수정해야 합니다.

7. **교정 조치.** 이 섹션에 의거하여 제공된 각 취약점에 대해 통지한 당사자는 Citi 에 대한 심각도 및 리스크를 토대로 해당 취약점의 리스크 수준 및 영향을 평가하고 그에 첨부된 부록에 명시된 CVSS(Common Vulnerability Scoring System)을 토대로 리스크 우선순위 수준을 지정해야 합니다. (<https://www.first.org/cvss> 참고) 리스크 수준이 지정되고 당사자 간에 합의에 이르면 공급업체는 식별된 중간, 높음 또는 심각 수준의 취약점을 교정해야 합니다. 가능한 경우, 이러한 취약점 교정 내용은 기존에 배포된 버전을 수정하는 보안 패키지 형태로 제공되어야 합니다.

공급업체가 Citi 가 만족할 만한 수준으로 취약점을 교정하지 못하거나 개선할 의사가 없는 경우, Citi 는 추가 책임이나 재정적 의무 없이 해당 라이선스를

해지할 수 있으며(해지된 부분에 대해), 공급업체는 이미 지급된 라이선스 수수료 중에서 비례 배분 후 남은 잔액을 즉시 Citi 에 환불해야 합니다.

17.44 커뮤니케이션 보안 네트워크 통제 기능

1. Citi 정보에 액세스하거나 Citi 정보를 저장, 관리, 처리 및/또는 전송하기 위해 사용되는 공급업체 네트워크는 반드시 위험으로부터 보호되어야 하고, 네트워크 내 시행 지점을 사용하여 정보 시스템의 보안을 유지해야 합니다.
 - a. 기밀 등급 이상의 Citi 정보는 인터넷 연결 비무장 지대(DMZ)에 있는 시스템에 지속적으로 저장되어서는 안 됩니다. 무단 접속을 방지하는 합리적인 통제를 포함한 무선랜(WLAN) 또는 기타 무선 기기 솔루션을 사용하여 Citi 정보에 액세스하거나 Citi 정보를 저장, 관리, 처리 및/또는 전송하는데 사용되는 네트워크는 Citi 정보가 포함된 네트워크에 연결될 수 있습니다.
 - b. 공급업체 글로벌 네트워크로의 모든 외부 IP 연결은 공급업체가 관리하는 방화벽에 의해 보호됩니다.
 - c. 실시간 침입 탐지 시스템(IDS) 및 침입 방지 시스템(IPS)을 갖추어 Citi 정보에 액세스하거나 Citi 정보를 관리, 저장, 처리 또는 전송하는 데 사용되는 공급업체 네트워크로의 인터넷 연결을 모니터링하고 보호합니다.
2. 모든 Citi 브랜드 인터넷 애플리케이션의 경우 공급업체는 다음을 보장해야 합니다.
 - a. 공급업체 사이트에서 호스팅되는 서비스는 Citi 가 승인한 DDoS(분산 서비스 거부) 방지 서비스나 Citi 에 의해 검증된 상응하는 수준의 통제 수단을 통해 보호됩니다.
 - b. 외부 방화벽은 기본적으로 거부(deny-by-default) 규칙으로 환경설정되어야 합니다. 방화벽 규칙은 최소 권한 원칙에 따라 구성되어야 하며 방화벽에 의해 거부된 모든 연결 시도(예: 패킷 삭제)는 로그/기록되어야 합니다.
 - c. 네트워크 통신 트래픽은 기본적으로 차단되고, 관리되는 인터페이스에서 예외적으로만 허용되어야 합니다. 예외 사항은 특정한 출처, 목적지 및 서비스에 한해 매우 제한적이어야 합니다.
 - d. 웹 애플리케이션 트래픽에는 웹 애플리케이션 방화벽(WAF) 등을 통한 적절한 통제 수단을 적용하고 필터링해야 합니다.

17.45 네트워크 분리

공급업체는 Citi 정보를 접근, 저장, 처리, 관리 및/또는 전송하는 데 사용되며 인터넷을 통해 접근 가능한 모든 정보 시스템 및 애플리케이션이 반드시 공급업체의 비무장 지대(DMZ)를 통해서만 접근되도록 해야 합니다.

비상 상황 발생 시 공급업체는 네트워크 보안 이벤트로 인한 영향을 줄이기 위해 네트워크 일부 간의 액세스를 필터링할 수 있어야 합니다(예: 바이러스 발생 시 포트 필터링).

원격 접속 및 호스트 보안은 공급업체 네트워크 내의 네트워크 리소스에 대한 접근을 제한하기 위해 그룹 기반 액세스 통제를 구현해야 합니다(예: 직원, 하청업체 등). 호스트 수준에서는 그룹이나 개인 수준에서 액세스 통제가 수행될 수 있습니다.

17.46 네트워크의 장비 식별

기술 플랫폼은 인터랙션 및 기타 완화 제어의 IS 리스크 수준에 상응하는 피어 기술 플랫폼을 식별하고 인증해야 합니다.

1. 본 요건을 충족하고 공급업체가 승인한 공급업체 기기(데스크톱, 노트북을 포함하되 그에 국한되지 않는 하드웨어)로만, Citi 정보가 저장되거나, 처리되거나, 전송되는 공급업체 네트워크에 액세스할 수 있습니다.
2. 이러한 요건을 준수하고 Citi 에서 승인한 공급업체 기기(예: 데스크톱, 노트북, 이동식 데이터 저장 매체를 포함하되 이에 국한되지 않는 하드웨어)만 Citi 네트워크에 액세스할 수 있습니다.

17.47 보안 요건 분석 및 사양

공급업체는 정보보안 절차를 애플리케이션, 제품 및 서비스의 선정, 개발 및 실행에 관한 과정 및 절차에 통합하여야 합니다.

17.48 온라인 거래

1. 해당되는 경우 공급업체는 자격을 입증하기 위하여 동적 비밀번호 또는 디지털 인증서를 사용하는 정보 시스템을 갖추어야 합니다.
2. 모든 최종 기관 인증서는 최소한 13 개월에 한 번씩 교체해야 합니다.
3. Citi 정보를 저장, 처리, 관리, 접속하는 공급업체 애플리케이션, Citi 브랜드의 인터넷 연결 애플리케이션을 호스팅하거나 Citi 의 네트워크 리소스에 연결되어 있는 공급업체 애플리케이션은 모두 다음을 준수해야 합니다.
 - a. 액세스하는 데이터/기능 유형에 따른 인증 방법을 활용해야 함
 - b. 다중 인증(MFA) 준수 평가를 수행하고 필요한 경우 권장 사항을 구현함
 - c. 의심스러운 활동 모니터링(SAM) 온보딩 평가를 수행하고 필요한 경우 권장 사항을 구현함
 - d. 이 모든 경우에 있어 공급업체는 주 비즈니스 담당자에게 연락하여 Citi 의 현재 요건에 대해 알아봐야 합니다.

17.49 통제 절차 변경

1. 공급업체는 방화벽, 침입탐지시스템(IDS) 및 침입방지시스템(IPS)에 대한 환경설정 변경이 공급업체의 변경관리절차를 통과하도록 해야 합니다.

2. 임시 ID 를 통하여 프로덕션에 승인된 접속은 환경에 대한 변경을 추적하기 위하여 기록하고 모니터하여야 합니다.
3. 기밀 등급 이상으로 Citi 정보로 분류되었거나, IS 리스크 요소 평가에서 “무결성” 또는 “높은” “가용성”으로 분류된 고객정보가 포함된 통제 정보 시스템과 관련하여 섹션 17.32(감사 기록)에 따라 캡처된 일지를 공급업체에서 검토해야 합니다. 이러한 검토는 적절한 위험에 기초한 표본조사법에 근거할 수 있습니다.
4. 검토는 임시 특권 접속의 일부인 변경 사항이 의도한 대로 만들어졌는지를 확인하여야 합니다.
5. 공급업체는 검토 과정의 증거를 보관하는 것을 포함하여 모든 변경 사항을 문서화해야 합니다.

17.50 정보 유출

공급업체는 다음을 포함한 정보유출을 방지하는 문서화된 보안 코딩 기준을 갖추어야 합니다.

1. 상세한 시스템 정보(예를 들면, 서버 유형 및 기술)
2. 디렉토리 트리 구조와 기본 데이터베이스 유형을 보여주는 스택 추적 및 예외 오류.

17.51 데이터 테스트

공급업체는 Citi 가 기밀 등급 이상의 정보로 분류한 정보를 산업 표준을 충족하는 도구와 방법을 사용하여 익명화, 마스킹 및/또는 난독화 처리하여 그러한 데이터가 더 이상 민감하지 않은 정보로 변경되거나 공급업체가 개발 또는 테스트 환경 내에서 실시간 프로덕션 제어를 구현하지 않는 한 그러한 기밀 등급 이상의 정보를 소프트웨어 애플리케이션 개발 환경이나 테스트 환경 또는 랩에서 사용하거나 저장해서는 안 됩니다.

17.52 시스템 수용

공급업체는 관련 업계의 기준을 충족하는 문서화된 프로젝트 범위 관리 및 시스템 수용 절차를 갖추어야 합니다.

17.53 정보 보안 취약점 보고

공급업체는 Citi 정보 자산에 대한 위협이 되는 애플리케이션 및 인프라 취약성이 **즉시 Citi 에 보고되도록** 하는 절차를 갖추어야 합니다.

17.54 보안 사고 책임 및 절차

1. SIRT 란 보안 사고가 발생한 방식이나 장소 또는 침해를 야기한 주체와 관계없이 다음 중 하나를 침해하는 보안 이벤트를 말합니다.

- Citi 데이터의 기밀성, 무결성 또는 가용성

- Citi 가 계약상, 법률상 또는 규제상 의무를 부담하는 모든 데이터(개인 정보 포함)의 기밀성, 무결성 또는 가용성
 - Citi 데이터를 저장, 처리 또는 전송하는 Citi 정보 시스템의 무결성 또는 가용성
2. 본 문서에서 기밀성 침해란 무단 사용자에게 데이터가 노출되는 경우 또는 Citi 가 데이터에 대한 보관 및 통제권을 상실하는 상황을 말합니다. 모든 보안 사고는 즉시 보고해야 합니다.
 3. 공급업체가 SIRT 를 경험한 경우, 공급업체는 Citi 의 자체 사고 대응 프로세스에 따라 Citi 가 요청하는 정보를 제공하고, Citi 가 법률상, 규제상 및/또는 내부 거버넌스 요건을 충족할 수 있을 정도로 침해된 데이터를 분석하는 데 Citi 와 협조해야 합니다. 또한 법률, 규칙 또는 규정에 따라 요구되거나 Citi 가 재량으로 원하는 모든 통지를 Citi 의 요청에 따라 공급업체의 비용으로 수행해야 합니다. 단, Citi 가 제안된 통지 양식의 문구를 검토하고 수정할 기회를 가진 후에만 통지할 수 있으며, Citi 가 서면으로 명시적으로 요청하지 않는 한 그러한 통지에 Citi 의 명칭을 언급해서는 안 됩니다.

17.55 데이터 유출 방지(DLP)

공급업체는 Citi 기밀 등급 이상의 데이터에 액세스 권한을 지닌 모든 직원을 포괄하는 엔드 포인트 모니터링을 포함하여 데이터 유출 방지(DLP) 통제 기능을 반드시 구현해야 합니다.

공급업체는 다음 채널을 통해 Citi 기밀 등급 이상의 데이터가 네트워크 밖으로 이동되는 것을 감지하고 방지하는 데 필요한 통제 기능을 갖추어야 합니다.

- a. 암호화되지 않은 이메일
- b. 암호화된 이메일 첨부 파일
- c. Citi 데이터 출력
- d. Citi 데이터를 네트워크 외부로 전송(예: FTP 를 통해).
- e. USB 드라이브, 외장 하드 드라이브, CD/DVD 드라이브 및 데이터 저장 기능이 있는 기타 외장형 기기와 같은 이동식 미디어에 Citi 기밀 등급 이상의 데이터를 복사하려는 시도. 이 권한은 기본적으로 방지되어야 합니다.
- f. DLP 솔루션은 Citi 기밀 등급 이상의 데이터를 네트워크에서 다른 목적지로 이동, 전송 또는 복사하려는 시도 (성공 여부에 관계없이)를 나타내는 모든 이벤트를 기록하고 이를 공급업체에 알려야 합니다. 이 권한은 기본적으로 차단되어야 합니다.
- g. SaaS/파일 공유 사이트를 포함한 외부 웹 사이트에 Citi 데이터 업로드 이 권한은 기본적으로 차단되어야 합니다.

17.56 웹 브라우징

1. 공급업체는 Citi 기밀 등급 이상의 정보를 공유하고 Citi 데이터에 액세스할 수 있는 직원이 악성 코드나 공격에 노출되는 것을 방지하는 데 필요한 웹 액세스 통제 기능을 갖추어야 합니다.
2. Citi 기밀 등급 이상의 데이터에 액세스 권한을 지닌 공급업체의 경우:
 - a. 모든 URL 요청을 반드시 기록해야 합니다.
 - b. Citi 데이터의 무단 공유(즉 웹 메일, 채팅, 소셜 미디어, 온라인 스토리지, Gen-AI 등)에 사용될 수 있는 사이트에 액세스하려는 시도는 차단되어야 합니다.
 - c. 환경을 맬웨어나 공격에 노출시킬 가능성이 있는 사이트에 대한 액세스를 차단해야 합니다.
 - d. 업무와 관련이 없는 것으로 간주되는 사이트에 액세스하려는 시도는 차단해야 합니다.
 - e. 공급업체는 정기적으로 업데이트되는 URL 분류 서비스(categorization service)를 구독해야 합니다. 분류되지 않은 모든 URL 은 기본적으로 차단하거나, 모든 URL 을 기본적으로 차단한 후 사례별로 승인해야 합니다.
 - f. 공급업체에서 사용 중인 웹 브라우저는 완전히 지원되어야 하고 소프트웨어 공급업체에서 제공하는 최신 보안 업데이트 버전으로 업데이트해야 합니다.

17.57 전자 메시징

인스턴트 메시징, P2P(피어투피어) 네트워크 또는 기타 인터넷 협업 도구는 섹션 17.9(암호 통제 사용 정책)에 따른 적절한 암호화 없이는 Citi 정보를 공급업체 네트워크 외부로 전송하거나 저장하기 위해 또는 Citi 정보가 있는 네트워크로부터 전송하거나 저장하기 위해 사용될 수 없습니다.

17.58 이메일

공급업체는 Citi 정보 공유와 맬웨어나 공격에 대한 노출을 방지할 이메일 통제 기능을 갖추어야 합니다. 다음 내용이 포함됩니다.

1. 이메일 게이트웨이를 통해 들어오는 첨부 파일이 시스템에 위험을 초래할 경우 스캔하고 차단해야 합니다.
2. 이메일 필터링(안티 스팸, 안티 피싱) 소프트웨어를 상시 사용하고 최신 버전으로 유지·관리해야 합니다.
3. Citi 의 기밀 등급 이상의 데이터가 공급업체의 조직 외부에 전송될 때는 반드시 암호화되어야 합니다.
4. 공급업체에서 사용하는 이메일 클라이언트 프로그램은 완전하게 지원되어야 하고 소프트웨어 공급업체에서 제공하는 최신 보안 업데이트 버전으로 업데이트해야 합니다.

17.59 이동식 미디어

1. 공급업체는 Citi 정보가 유지 관리되는 매체에 상관 없이 Citi 정보를 반드시 보호해야 합니다. 이 표준은 정보가 저장된 다음 유형의 매체에 적용되지만, 이에 국한되지는 않습니다. 카드, 카세트, CD, 체크 스톱, 디스켓 또는 삭제 가능한 그 외의 저장 기기, 인쇄물, 자기 디스크, 자기 테이프, 마이크로 필름, 마이크로피시, 광디스크 또는 종이 문서 등이 포함됩니다.
2. Citi 정보가 저장되어 있는 시스템에 대한 이동식 매체/저장 기기의 접속 초기 설정은 반드시 접근 금지여야 합니다. 예외가 허용되어 읽기-쓰기 액세스가 허용되는 경우 해당 데이터는 휴대용 저장 기기에 암호화된 상태로 저장되어야 합니다.
3. 이동식 매체 사용을 허용하는 경우, 경영진이 반드시 그러한 매체의 사용을 승인해야 하며, 비즈니스에 이동식 매체 사용이 필요한 근거를 포함해야 합니다. 이동식 미디어는 관리자에 의해 목록화되어야 합니다. Citi의 기밀 등급 이상의 데이터가 담긴 이동식 매체는 사용자가 별도 조치하지 않더라도 자동으로 암호화되는 기능을 갖춰야 합니다.

17.60 매체 폐기

1. Citi 분류 등급상 기밀 등급 이상으로 분류된 Citi 정보가 Citi의 지시에 따라 폐기되어야 하는 경우에는 (즉, 정보가 더 이상 Citi에게 필요치 않거나 무익할 때, 그리고 법, 규정 및/또는 Citi 정책이 요구하는 추가적인 보유 기간이 만료되었을 때) 공급업체는 그러한 정보를 사용할 수 없고 복구를 불가능하게 하는 방법으로 파기해야 합니다.
2. 다음 규칙에 따라 데이터 탑재가 가능한 매체를 안전하게 지울 때는 다양한 특정 문자를 사용해 드라이브 섹터를 무작위로 덮어 쓰는 승인된 도구를 사용해야 합니다.
 - a. 기밀 또는 그 이상의 등급으로 분류된 정보를 저장하는 매체의 경우, 해당 도구는 매체에 대해 3회 덮어쓰기 작업을 완료해야 합니다.
 - b. 매체를 디가우싱합니다(해당되는 경우).
3. 해당 미디어를 읽을 수 없게 물리적으로 파기합니다(예: 파쇄, 드라이브 분쇄).
4. 기밀 등급 이상의 정보가 담긴 종이 및 기타 비전자적 저장 매체는 최종 폐기 전에 안전하게 수거하여 안전한 "기밀 보관함"에 보관해야 합니다. 기밀 보관함은 항상 잠겨 있어야 하며 권한이 있는 사람만 열 수 있어야 합니다.
 - a. 복사기, 프린터, 팩스 기계 및 Citi 기밀 등급 이상의 정보가 담겨 있을 가능성이 있는 메모리/저장 기기가 있는 일체의 다른 기기에서도 기밀 정보를 깨끗이 지워야 합니다.

17.61 정보 보안 관리 및 교육

1. 피싱 및 기타 사회공학적 공격 방지, 기밀 이상 정보의 적절한 처리, 보안 사고 보고 및 대응 관리 등을 포함하되 이에 국한되지 않는 적절한 사이버/정보 보안 인식 및 교육 프로그램을 유지합니다.
2. 공급업체는 계약직 및 임시 직원을 포함한 모든 직원이 본인의 직무와 관련한 회사 정책과 절차에 관한 적절한 의식 강화 교육을 반드시 실시해야 합니다.
3. 공급업체는 새롭게 대두되는 리스크와 위협, 최신 모범 사례, 사이버 보안 환경의 신기술을 반영할 수 있도록 교육 및 인식 제고 프로그램을 매년 검토하고 업데이트해야 합니다.
4. 해당 교육에서는 최소한 다음의 다양한 주제를 반드시 포함해야 합니다.
 - b. 정보 라벨링 및 취급
 - c. 안전한 전송(보안 이메일, 안전한 SharePoint 저장, Citi 소유 데이터의 개인 이메일 전송 금지)
 - d. 정보 보안 사고 신고
 - e. 안전한 업무 환경(예: 적절한 인터넷 사용, 무단 소프트웨어, 승인되지 않은 소프트웨어 다운로드 금지)
 - f. 비밀번호 관리(예: 강력한 비밀번호, 비밀번호 공유 금지)
 - g. 사회 공학(예: 피싱, 스피어 피싱, 비싱, 스미싱)
 - h. 원격 근무(예: 보안/안전 연결, 개인 기기 보안)
5. 공급업체 직원은 Citi 데이터를 호스팅하는 시스템에 액세스하기 전에 교육을 배정받아야 하며, 배정 알림에 명시된 기한까지 교육을 완료해야 합니다.
 - a. IS 교육은 법에서 금지하지 않는 경우 최소한 매년 모든 직원에게 실시되어야 합니다.
6. 현지 법률이 허용하는 경우, 교육에는 교육 효과를 측정한 결과를 기록하는 산출물(예: 수료 시 통과/실패 기준 점수가 있는 퀴즈)을 포함해야 합니다.

17.62 사이버 리스크 관리 프로그램

또한, 공급업체는 최소한 다음 방법을 포함하는 적절한 사이버 리스크 관리 프로그램을 유지·관리해야 합니다.

1. 잘 정의되고 문서화된 정보 보안 위험 관리 프로그램 및/또는 명확하게 정의된 사이버/정보 위험 관리 구성 요소가 있는 운영 위험 관리 프로그램을 유지하여 공급업체의 사이버 위험 성향을 정의하고 사이버 잔존 위험이 해당 위험 성향에 부합하도록 보장합니다.
2. 조직 내 전반적인 보안 상태를 평가하는 보안 감사 및 검토의 수집 및/또는 수행을 포함하되 이에 국한되지 않는 강력한 보안 위험 관리 거버넌스 프로그램을 유지하고, 적어도 매년 경영진에게 보고하여 공급업체의 사이버 위험 성향이 위반되지 않았는지 검토하고 보증합니다.

3. 공급업체가 신용/직불 카드 거래, 결제 및/또는 정보를 처리, 저장 및/또는 전송하는 경우 공급업체에 적용되는 모든 PCI 데이터 보안 표준(PCI-DSS)을 준수합니다.
4. 공급업체가 시도되거나 의심되거나 실제로 발생한 모든 사이버 보안을 감지, 억제, 조사, 대응 및 복구할 수 있는 충분하고 적절한 역량을 갖추도록 업계 표준에 따라 위기 관리 계획 및 플레이북과 보안 사고 대응팀 계획을 유지해야 합니다.

17.63 애플리케이션, API, 코드, 시스템 및 인프라 보안

공급업체가 개발 환경을 호스팅, 개발, 공동 개발, 제공 및/또는 소프트웨어 애플리케이션을 제공하는 경우, 공급업체는 해당 소프트웨어 및/또는 소프트웨어 패치의 코드 검토 작업을 수행해야 합니다. 이 작업에서는 보안 결함, 무단 액세스, 수정 및/또는 맬웨어나 기타 형태의 악성 코드 삽입 방지 기능을 검토하는 동시에, 애플리케이션(API 포함)과 기초 시스템 서비스, 운영체제, 그리고 보안 사고, 개인정보 유출, 사기, 무단 액세스 및/또는 기밀정보 공개, 해당 애플리케이션에 의해 처리, 저장, 전송되는 정보의 무결성 훼손 및/또는 공급업체가 Citi에 제공하는 제품 및/또는 서비스의 품질에 영향을 미칠 수 있는 가용성 손실로 이어질 가능성이 있는 식별된 네트워크 취약성과 결함이 없음을 확인해야 합니다.

17.64 모바일 보안

공급업체가 모바일 어플리케이션 솔루션을 제공하는 경우 공급업체는 다음 요건을 준수해야 합니다.

1. 모바일 애플리케이션은 Google Android(Android Go 제외) 및/또는 Apple iOS/iPadOS 플랫폼의 일반적으로 사용 가능한(GA) / 안정된 버전 및 비 EOL² 버전만 지원해야 합니다. 모바일 솔루션에 추가 지원을 제공하는 경우, 지원되는 운영 체제/버전은 Citi에서 구성할 수 있어야 합니다
2. 모바일 솔루션은 이 문서의 섹션 17.9(암호화 요건)에 명시된 암호화 기능을 포함하되 이에 국한되지 않는 암호화 알고리즘을 지원하는 일반적인 지침 세트가 없는 모바일 플랫폼/기기를 지원해서는 안 됩니다.
3. 베타 버전, 얼리 액세스 버전, 기능 미리보기 버전/릴리스 등 사전 프로덕션 운영 체제 버전은 프로덕션 환경에서 허용되지 않습니다.
4. 공급업체는 모바일 솔루션에 의해 번들로 제공되거나 활용되는 무료 및 오픈 소스 소프트웨어 라이브러리 등 통합된 제 3 자 구성 요소 목록을 제공할 수 있어야 합니다.
5. 모바일 애플리케이션은 Apple App Store 또는 Google Play 스토어와 같은 공개 앱 스토어를 통해 모바일 애플리케이션을 게시할 수 있는 요건과 모범 사례를 준수해야 합니다. 나열된 공개 애플리케이션 스토어는 모바일

² 플랫폼 소유자 또는 공급업체로부터 정기적인 보안 및 유지보수 업데이트를 받고 있는, 현재 지원 중인 제품 버전.

애플리케이션을 배포/게시하는 데 가장 우선적이고 주요한 수단이어야 합니다.

6. Android 모바일 애플리케이션은 APK 서명 체계 v2+를 사용해야 합니다. APK 서명 체계 버전 1(JAR 서명이라고도 함)을 사용하면 안 됩니다.
7. 모바일 애플리케이션 서명 키 유형 및 길이는 이 문서의 섹션 17.9 – 암호화 요건을 준수해야 합니다.
8. 각 애플리케이션 서명 키 및 관련 X.509v3 인증서는 개별적으로 관리되어야 하며 단일 애플리케이션 ID/변들 ID 에 전용되어야 합니다. 서명 키는 애플리케이션 간에 공유해서는 안 됩니다.
9. 모바일 애플리케이션이 모바일 기기의 데이터를 보관해야 하는 경우, 앱/서비스의 목적을 위해 필요한 최신 데이터만 기기에 보관하거나 법률 또는 규제 요구 사항에 따라 필요한 경우에만 보관해야 합니다.
 - a. 사용자 데이터의 수집, 처리 및/또는 저장은 일반 데이터 보호 규정(GDPR) 및 2002/58/EC(ePrivacy) 지침 또는 지역별 동등 조항과 같은 개인정보 보호 규정 등의 현지 법률을 준수해야 합니다.
 - b. 통합된 제 3 자 구성요소(예: 라이브러리)는 사용자 데이터를 수집, 처리 및/또는 저장해서는 안 됩니다.
10. 모바일 애플리케이션은 권한이 없는 사용자가 애플리케이션 데이터에 액세스할 수 없도록 해야 합니다.
 - a. 다른 애플리케이션과 데이터를 공유해야 하는 경우, 애플리케이션은 해당 운영 체제에 상업적으로 합리적인 기술, 방법 및 통제 기능을 활용하여 이러한 데이터 공유가 적절히 정당화되고 문서화된 경우에 최소한의 다른 애플리케이션과 필요한 양의 데이터만 공유해야 합니다.
11. 모바일 애플리케이션은 각 모바일 운영 체제에서 제공하는 안전한 통신 시설에만 의존해야 합니다. 예:
 - a. Android 애플리케이션은 애플리케이션 매니페스트 및/또는 네트워크 구성 파일에서 보안되지 않은 네트워크 트래픽이 어떠한 네트워크 도메인으로든 허용되지 않는다는 것을 명시적으로 선언해야 합니다.
 - b. iOS/iPadOS 애플리케이션은 예외 없이 애플리케이션 전송 보안(ATS)을 사용해야 합니다.
12. 암호화 자료는 하드웨어가 지원하는 안전한 키 저장소에 바인딩되어야 합니다.
13. 모바일 애플리케이션은 릴리스 모드로 구축되어야 하며 다음을 포함해서는 안 됩니다.
 - a. 보안 통제를 우회할 수 있는 모든 기능 또는 방법,
 - b. 리버스 엔지니어링을 용이하게 할 가능성이 있는 소스 코드 파일 이름, 변수 이름, 기호 이름, 주석 등과 같은 디버그 정보.

14. 모바일 애플리케이션에는 런타임에 애플리케이션의 동작을 변경하거나 모니터링할 수 있는 악성 코드 삽입을 방지하기 위해 효과적인 안티 후킹 또는 안티 변조 메커니즘이 갖춰져야 합니다.
15. 모바일 애플리케이션은 리버스 엔지니어링 공격을 방해하기 위해 포괄적인 안티 디버깅 또는 안티 리버스 엔지니어링/난독화 기술을 구현해야 합니다.
16. 모바일 애플리케이션 패키지는 콘텐츠의 진위성과 무결성을 확인할 수 있는 기능을 갖춰야 합니다(예: 암호화 체크섬 및/또는 디지털 서명 사용).
17. 모바일 애플리케이션이 사용자 인증을 필요로 하는 경우, 애플리케이션 및/또는 기기 무결성 확인은 사용자 인증이 시작되기 전에 완료되어야 합니다.
18. Citi 가 소유한 정보 중 기밀 등급 이상으로 분류되었거나 IS 리스크 분류가 Medium 이상으로 분류된 정보를 액세스/처리/저장하는 모바일 애플리케이션은 강력한 생체 인식 방식만 사용해야 합니다(예: 해당 [Android Compatibility Definition Document](#) 에 정의된 클래스 3/강력 범주를 충족하거나 능가).
19. 모바일 애플리케이션은 중간자 공격(MitM)을 방지하기 위한 대책을 구현해야 합니다.
20. 모바일 애플리케이션은 '탈옥' 또는 '루팅'된 모바일 기기를 포함하되 이에 국한되지 않는 손상된 기기를 감지하고 기업의 위험 평가 및 규제 요구 사항에 따라 대응할 수 있어야 합니다.
21. 모바일 애플리케이션은 소프트웨어 토큰(예: 소유 증명)이 복제되는 것을 방지하기 위해 강력한 기기 바인딩을 구현해야 합니다.
22. 모바일 애플리케이션은 안전한 키보드 애플리케이션/솔루션(예: 모바일 운영 체제에 기본 제공/사전 설치된 애플리케이션)을 사용해야 합니다.
23. 푸시 알림에는 민감한 정보(예: 기밀 등급 이상으로 분류된 Citi 정보)가 포함되어서는 안 됩니다. 하지만 일회용 비밀번호(OTP)는 푸시 알림을 통해 배포될 수 있습니다.
24. 모바일 애플리케이션 솔루션은 알려지거나 악용될 수 있는 취약점이 있는 애플리케이션 버전을 사용하는 모바일 클라이언트와의 통신 시도를 거부/무시할 수 있는 기능을 갖춰야 합니다.
25. 모바일 애플리케이션은 [OWASP Mobile Top 10](#) 에 게시된 예방 기술을 포함하되 이에 국한되지 않는 업계 모범 사례를 준수해야 합니다.
26. 인공 지능 및 머신 러닝(AI/ML) 기술을 활용하는 모바일 애플리케이션은 윤리적으로, 그리고 섹션 19 – **Error! Reference source not found.**(생성형 AI/에이전트형 AI 포함)에 따라 이를 수행해야 합니다.
27. 모바일 애플리케이션은 Citi 에서 활용하는 목적/기능을 수행하는 데 필요한 최소한의 기기 권한을 활용해야 합니다.
28. 모바일 애플리케이션은 SD 카드와 같은 외부/이동식 저장 기기에 비공개 정보를 저장해서는 안 됩니다.

Error! Reference source not found.**Error! Reference source not found.**

17.65 소프트웨어 공개

공급업체는 Citi 에 제공하는 모든 제품 또는 서비스에 포함된 오픈 소스 소프트웨어 등을 포함하되 이에 국한되지 않는 모든 소프트웨어 구성 요소(총칭하여 ‘소프트웨어 구성 요소’)를 공개해야 합니다. 공급업체는 Citi 에 사전에 공개하지 않고는 Citi 시스템에 설치될 제품 또는 서비스의 어떠한 버전에도 업데이트, 업그레이드 또는 기타 방법으로 소프트웨어 구성 요소를 통합하지 않습니다. 또한 공급업체는 자사의 제품이나 서비스에 Citi 또는 그 계열사가 Citi 와의 계약에서 명시적으로 공개 및 수락하지 않은 의무를 지도록 하는 조건에 따라 라이선스가 부여된 소프트웨어 구성 요소가 포함되지 않도록 보장해야 합니다. 공급업체는 자사 조직, 제품 또는 서비스 내에서 발견된 모든 악성 소프트웨어 구성 요소를 발견일로부터 30 일 이내에 Citi 에 공개해야 합니다. 구체적으로 공급업체는 OWASP CycloneDX 파일 형식이나 ISO/IEC 5962:2021 소프트웨어 패키지 데이터 교환(SPDX) 사양 파일 형식의 소프트웨어 구성표(SBOM)를 Citi 에 제공하여 제품 또는 서비스의 각 릴리스 및 버전에서 소프트웨어 구성 요소 사용을 공개해야 합니다. 이러한 공개에는 소프트웨어 구성 요소의 출처(예: 상용 공급업체, 내장 데이터베이스, 공개 바이너리 패키지 관리자, 소스 코드에서 빌드된 구성 요소, 임베디드 소프트웨어 또는 선별된 소프트웨어 구성 요소 제공업체)와, 공급업체 또는 그 소프트웨어 공급망 종속성 중 어느 하나가 해당 소프트웨어 구성 요소의 사본(‘포크’)을 생성한 후 패키지 종속성 또는 제품 및 서비스를 컴파일하는 공급업체의 소스 코드에 통합된 소스 코드로서 이를 자사의 제품 또는 서비스에 빌드했는지 여부를 포함해야 합니다.

17.66 위험 모델링

공급업체는 다음을 모두 포괄적으로 다루고(다루거나) 포함하는 위험 모델링리 프로세스를 구현해야 합니다.

1. 범위 정의: 공급업체는 Citi 의 기밀 또는 그 이상의 등급 정보를 처리, 저장 또는 전송하는 소프트웨어 구성 요소 및 데이터 흐름에 중점을 두어 위험 모델의 범위를 명확히 정의해야 합니다.
2. 위험 식별: 공급업체는 설계 수명 주기 초기 단계에서 다양한 공격 벡터와 위험 행위자를 고려하여 소프트웨어의 설계, 아키텍처, 의도된 용도와 관련된 잠재적 위험 및 취약성을 체계적으로 식별해야 합니다.
3. 리스크 분석: 공급업체는 식별된 위험의 잠재적 영향 및 발생 가능성을 분석하여 보안 리스크의 우선순위를 정할 수 있어야 합니다.
4. 통제 수단 통합: 공급업체는 우선순위가 정해진 리스크를 해결하기 위해 적절한 보안 통제 수단 및 경감 전략을 소프트웨어 설계 및 개발 과정에 정의하고 통합해야 합니다.
5. 문서화: 공급업체는 식별된 위험, 관련 리스크, 해당 완화 조치를 포함하여 위험 모델을 문서화해야 합니다.
6. 정기 검토: 공급업체는 특히 소프트웨어의 설계, 기능 또는 배포 환경에 중대한 변경이 있는 경우 위험 모델을 정기적으로 검토하고 업데이트해야 합니다.

17.67인공 지능

1. 공급업체는 Citi 에 제공되거나 Citi 와 통합되는 모든 AI/ML 시스템 및 구성 요소에 대해 견고한 보안 소프트웨어 개발 수명 주기(SSDLC)를 구현하고 준수해야 합니다. 여기에는 안전한 설계, 개발, 테스트, 배포, 지속적인 유지 관리가 포함됩니다.
2. 공급업체가 제공하는 AI 시스템은 운영의 무결성을 입증하고 적대적 공격에 대한 견고한 저항력을 보여야 합니다. 여기에는 프롬프트 인젝션 탐지, 입력값 정제, 데이터 격리 유지 메커니즘의 구현이 포함됩니다.
3. 공급업체가 제공하는 AI 에이전트 및 구성 요소는 Citi 시스템 및 기타 도구와 안전하게 상호 작용해야 합니다. 이를 위해서는 강력한 ID 및 액세스 관리, 도구 실행 인수의 엄격한 검증 및 고위험 도구 작업의 격리가 필요합니다. 민감하거나 고위험인 작업에는 인간 개입(Human-in-the-Loop, HITL) 메커니즘을 포함해야 합니다.
4. 공급업체 AI 시스템은 모든 중요한 이벤트에 대해 포괄적이고 변경 불가능하며 감사 가능한 로그를 생성해야 합니다. 이러한 로그는 변조로부터 보호하고 집계해야 하며 Citi 정책에 따라 보존해야 합니다. 보안 관련 사고 및 의심스러운 활동을 식별하고 경고하기 위한 지속적인 모니터링 및 이상 탐지 기능이 필요합니다.
5. 공급업체 AI 시스템은 적절한 개입이 가능하도록 리스크 기반의 사람 감독을 지원하고, AI 결과물 및 조치에 대한 명확한 책임성을 갖도록 설계해야 합니다. 여기에는 AI 결과물을 리스크 수준별로 분류하고 사람의 재정의 기능을 지원하는 것이 포함됩니다.
6. 공급업체가 제공하는 모든 AI 에이전트, 구성 요소, 시스템은 견고한 ID 및 액세스 관리 통제 수단을 구현해야 합니다. 모든 AI 상호 작용은 식별 가능한 ID(사람 또는 비인간)에 귀속될 수 있어야 하며, 모든 액세스에는 인증이 필요합니다. AI 담당자는 Citi 리소스에 액세스할 때 관리형 ID 를 사용하고 최소 권한 원칙을 따라야 합니다.
 - a. 공급업체는 Citi 보안 정책 적용, 중앙 집중식 ID 관리, 감사 가능성을 지원하도록 모든 AI 담당자에 Citi ID 및 액세스 관리(IAM) 시스템과 연동되는 Citi Object Identity Network(COIN) 에이전트 ID 를 할당하고 이를 보장해야 합니다.
 - b. 공급업체는 보안 게이트웨이(SSG Gateway 또는 Apigee)를 통해 제공되는 COIN API 를 포함하여 Citi 가 승인한 통합 메커니즘을 사용해 제 3 자 에이전트를 COIN 에 온보딩해야 하며, 이러한 온보딩이 Citi 의 적용 보안 요건에 따라 안전한 방식으로 수행되도록 보장해야 합니다.
 - c. 내부에 호스팅되는 공급업체는 COIN 에 부합하는 자체 토큰을 생성해야 합니다. 외부에 호스팅되어 자체 연동 토큰으로 인바운드 인증을 수행하는 공급업체는 Microsoft 토큰을 COIN 토큰으로 교환하는 방식과 같이 Citi 토큰으로 교환할 수 있도록 지원되는 교환

토큰을 보유해야 합니다. 현재 교환을 통해 지원되지 않는 모든 신규 토큰 유형은 Citi IAM 팀의 승인을 위해 검토해야 합니다.

7. 공급업체가 모델 컨텍스트 프로토콜(MCP) 서버 또는 클라이언트를 사용하거나 제공하는 경우, 모든 선택 기능을 포함하여 MCP RFC 7591 을 구현해야 합니다.
8. 공급업체 AI 시스템은 시스템 프롬프트 및 내부 작동 방식이 공개되거나 조작되지 않도록 보호해야 합니다. 컨텍스트 관리는 테넌트, 사용자 또는 환경 간 데이터 유출을 방지하기 위해 엄격한 경계를 적용해야 합니다.
9. 공급업체는 적대적 공격, 모델 조작, 무단 AI 조치 또는 AI 시스템 관련 데이터 침해를 포함한 AI 특화 보안 사고를 탐지, 대응 및 보고하기 위한 문서화된 절차를 마련해야 합니다. 이러한 사고 발생 시, Citi 에 즉시 통지해야 합니다.

18 보안 작업장 지침

Citi 정보에 액세스하거나 Citi 정보를 처리/관리/저장하는 공급업체 및/또는 Citi 브랜드의 인터넷 기반 애플리케이션을 호스팅하는 공급업체 및/또는 Citi 의 네트워크 리소스에 연결된 공급업체 및/또는 Citi 시설에 동반자 없이 액세스해야 하는 공급업체에 적용.

공급업체는 Citi 와 Citi 고객의 유형 및 무형 자산을 보호해야 합니다. Citi 와 고객 자산은 승인된 목적과 방식으로만(예: 해당 라이선스, 약관에 따라) 사용될 수 있으며, Citi 와 Citi 공급업체의 비즈니스 목적과 관련해서만 사용될 수 있습니다. 자산은 현금, 증권, 실물 재산, 서비스, 사업계획, Citi 정보, 공급업체 정보, 판매자 정보, 지적재산권(컴퓨터 프로그램, 모델과 기타 품목), 기타 모든 사적, 독점 및 기밀 정보를 포함합니다. Citi 자산의 남용이나 무단 공개는 Citi 에 대한 의무의 위반이며 Citi 에 대한 사기행위가 성립될 수도 있습니다. 유사하게, Citi 자산에 대한 부주의, 낭비 또는 무단 사용 역시 Citi 에 대한 의무의 위반입니다.

항목	요건
Citi 정보(전자 및 출력 문서)	정상 근무시간 이후에는 물론, 공급업체가 지정된 작업 공간을 비울 시에는 Citi 정보를 잠그고 안전하게 보관하십시오.
데스크톱 개인용 컴퓨터(PC) 및 노트북	Citi 정보에 접속하거나 열람하기 위해 사용하는 PC 와 노트북은 일정 시간 동안 사용하지 않을 경우 화면 보호기 비밀번호로 보호해야 합니다. 공급업체가 지정된 작업 공간을 벗어날 때마다 CTRL + ALT + DEL 을 눌러 PC 및/또는 노트북을 잠그고 "컴퓨터 잠금"을 선택해야 합니다. 공급업체가 Citi 정보를 보기 위해 노트북을 사용하는 경우, 근무 시간 중에는 해당 노트북을 본체에 케이블 또는 보안 잠금 기기로 고정하고, 근무 시간이 끝난 후에는 안전하게 잠가 보관해야 합니다.
잠금	Citi 정보를 저장하는 파일 캐비닛과 서랍은 정상 근무시간 후에는 반드시 잠가야 합니다.

항목	요건
개방된 사무실 구역	Citi 정보를 저장하기 위한 파일 서버/미니 데이터 센터로 사용되기 위해 특별히 설계되고 Citi 에 문서화된 경우가 아니라면 개방된 사무실 구역을 이러한 목적으로 사용해서는 안 됩니다.
프린터, 복사기 및 팩스 트레이	모든 Citi 관련 자료는 프린터, 복사기 및 팩스 트레이에서 치워야 합니다.
폐기	더 이상 필요치 않은 Citi 정보는 폐기하여야 합니다(특정 보존 기한 준수). 문서는 분쇄하거나 보안이 유지된 잠금식 재활용함에 넣어야 합니다. 자기 매체는 반드시 적절한 삭제 절차를 따른 후 안전하게 폐기하여야 합니다.

19 인공 지능/머신 러닝(생성형 AI/에이전트형 AI 포함)

제공하는 제품/서비스의 일체 부분에서 Citi 가 이러한 공급업체 요건들을 통해 정의한 인공지능 및 머신 러닝(AI/ML)(생성형 AI/에이전트형 AI 포함)을 활용하는 공급업체에 적용됩니다.

19.1 공급업체는 계약에 따른 해당 별첨 또는 작업 지시서에서 당사자 간에 그러한 사용에 합의하지 않은 한, 아래에 설명된 AI/ML 을 사용해서는 안 되며, 하청업체도 사용하지 않도록 보장해야 합니다.

- a. AI/ML 이 Citi 에 직간접적으로 제공하기로 계약을 체결한 제품이나 서비스에 사용되거나, 포함되거나, 달리 통합되거나, 그의 일부분인 경우(일체의 제 3 자 제품·서비스 포함), 또는
2. AI/ML 이 공급업체의 일체 계약 이행에 어떤 형태로든 활용되는 경우, 그러한 AI/ML 이 Citi 에 제공 중인 실제 제품·서비스에 사용되거나, 포함되거나, 달리 통합되었는지 여부, 또는
3. AI/ML 이 공급업체에 의해 어떤 형태로든 활용됨으로써 Citi 정보가 그러한 AI/ML 에 노출될 수 있는지에 대한 설명. 여기에는 공급업체가 비상업적 비즈니스 운영 활동(예: 비즈니스 기록 보관, 프로세스 개선, 연구·개발, 규정 준수, 내부 감사) 시 활용하는 일체의 AI/ML 이 포함되며, 그에 국한되지 않음.

19.2 공급업체가 이러한 의무를 준수하지 못하는 경우 본 계약 조건의 중대한 위반으로 간주됩니다.

19.3 상품/서비스의 일체 부분에서 AI/ML 사용에 대한 규제 관련 검사 또는 포렌식 조사의 일환으로, 규제기관이 요청하는 경우, 공급업체는 Citi 가 규제 기관의 요청에 응답하는 과정에서 협조해야 합니다. 여기에는 해당 AI/ML 모델을 구성하는 알고리즘의 실제 작동법을 확인하는 데 필요한 알고리즘 감사 작업의 수행 및/또는 수행을 진행할 수 있도록 돕는 것이 포함됩니다.

19.4 또한, 다음 원칙도 반드시 준수해야 합니다.

합법성. 공급업체 AI/ML 은 관련 법률을 준수해야 합니다.

목적 및 비례성. 공급업체는 콘텐츠나 Citi 정보를 공급업체나 제 3 자 데이터와 병합할 수 없습니다. 공급업체는 Citi 의 서면 승인 없이 콘텐츠 또는 Citi 정보를 사용하여 AI/ML 을 훈련할 수 없습니다. 공급업체 AI/ML 은 서비스 제공에 필요한 범위를 제외하고는 콘텐츠나 Citi 정보를 사용할 수 없습니다.

20 고객 불만

20.1 불만 사항은 고객, 비교객, 잠재 고객, Citi 클라이언트, 잠재 클라이언트 또는 클라이언트의 공인 대리인(총칭하여 "고객")이 Citi 정책, Citi 에서 제공하는 또는 Citi 를 통해 제공되는 상품 및 서비스, Citi 직원, Citi 하청업체 또는 Citi 를 대신하여 행동하는 제 3 자 서비스 제공자 또는 이들의 조합에 대해 불만을 표현하는 구두 또는 서면 의사소통으로, 구두(직접 또는 전화) 또는 서면(우편 또는 이메일, 채팅, 소셜 미디어 등의 전자 의사소통을 통해)으로 접수할 수 있습니다.

20.2 공급업체는 Citi 고객 불만 처리 정책 및 해당되는 Citi 불만 관련 표준 및 절차를 준수해야 합니다. 공급업체는 Citi 를 대신하여 제공하는 서비스와 관련되거나 그 밖에 Citi 와 관련하여 고객(또는 Citi 불만 정의에 따른 비교객 또는 잠재 고객) 또는 규제 기관으로부터 서면 또는 구두로 제기된 불만족 또는 우려 사항(각각 '불만')을 접수한 경우, 24 시간 이내에 이를 서면으로 주된 Citi 비즈니스 담당자(또는 지정인)에게 통지해야 합니다. Citi 가 해당 시스템을 공급업체에 제공하지 않는 한, 공급업체는 불만 사항을 추적할 수 있는, Citi 가 합리적으로 만족할 만한 시스템("추적 시스템")을 자체적으로 개발, 구현 및 유지해야 하며, Citi 의 재량에 따라 해당 시스템에 대한 보고서 사본을 제공하거나 시스템 접근 권한을 제공해야 합니다. 추적 시스템은 다음을 수행합니다.

- a. 불만 접수 건을 유형, 접수일, Citi 에 불만 통지 사실을 알린 날짜별로 분류.
- b. 불만 처리 과정을 결론/해결까지 추적
- c. Citi 가 합리적으로 요청하는 모든 기타 사항 처리. 추적 시스템은 공급업체가 특정 사안에 대해 과도한 수의 불만이 접수되는지 확인할 수 있도록 설계되어야 하며, 이를 통해 공급업체는 (Citi 와 협의하여) 공급업체의 비즈니스나 서비스 제공과 관련된 시스템적인 문제가 있는지 확인하고 신속하게 문제를 수정할 수 있습니다.

21 개인 거래 및 투자 정책

Citi의 개인 거래 및 투자 정책(Personal Trading and Investment Policy, PTIP)은 허용 및 금지된 거래 및 투자 활동, 사전 승인 요건, 그리고 적용 대상자의 중개 또는 거래 계좌의 유지, 공개 및 감시와 관련된 요건을 정의합니다. 여기에는 (1) Citi 또는 제 3자에 관한 중요 비공개 정보 또는 내부 정보(이하 'MNPI'), 또는 (2) 고객의 증권, 파생상품 및 상품 포지션, 거래 및 전략에 관한 정보를 포함하여 개인의 지위 또는 Citi와의 관계가 부적절하게 사용되는 것을 방지하기 위한 법률 및 규정 준수를 촉진하기 위한 최소 기준이 제시됩니다.

Citi에서 직무상 MNPI에 정기적으로 접근해야 하는 모든 공급업체 직원은 적용 대상자 및/또는 Citi 액세스 담당자로 지정되어 PTIP의 요구 사항을 준수해야 합니다. 공급업체 직원은 개인 계좌 공개, 개인 거래 활동 사전 승인, 개인 거래 제한, 정기 명세서 제출과 관련된 ICRM의 요청을 준수해야 합니다.

22 청구 및 송장 표준

Citi의 서비스 신속성 개선 및 통제 강화 노력과 관련하여, 모든 공급업체는 아래에 상세히 설명된 Citi의 송장 제출 선호 방식 및 송장 결제 선호 옵션을 지원해야 합니다.

- 공급업체는 Citi가 공급업체에 전달한 형식으로 Citi에 전송할 전자 파일을 생성하고/또는 Citi iSupplier 도구를 활용하여 필요한 송장/청구 데이터를 입력한 후 Citi에 디지털로 전송합니다.
- 공급업체는 전자 결제를 원활히 진행할 수 있도록 Citi에 필요한 모든 은행 정보 및 관련 서류를 제공하고, (가능한 경우) Citi의 가상 카드 결제 수단을 활용해야 합니다.

참고: 지급 조건은 Citi에서 송장을 접수한 날짜부터 계산됩니다.

적시에 지불하고 계약상의 의무를 이행하기 위해 Citi는 모든 공급업체가 Citi에 상품이나 서비스에 대한 청구서를 보낼 때 다음의 송장 데이터를 포함하고 관련 지침을 준수하도록 요구합니다.

1. 올바른 Citi 사업 법인명, “청구지” 주소, 및 관련된 Citi 비즈니스 담당자 이름.
2. 송장 번호, 송장 날짜 및 구매 주문서 번호.
3. 송장은 Citi 구매 주문서에 명시된 Citi 지점이나 이메일 주소로 보내야 합니다.
4. 청구되는 상품이나 서비스에 대한 명확하고 설명적인 세부 정보가 송장 내에 포함되어야 합니다.
5. 해당 송장에 대한 현재 요금만 포함합니다(기타 미지불 보류 송장 잔액은 포함하지 않습니다).
6. 송장은 증빙 서류를 포함하여 모두 영어로 작성되어야 합니다.

23 의무 휴가 정책

Citi의 의무 휴가 정책에 따라, 특히 회사의 장부 및 기록에 영향을 미치는 민감하거나 고위험 활동을 수행하는 개인은 해당 업무에서 정기적으로 벗어나야 합니다. 이러한 의무적 업무 분리는 내부 통제를 강화하고, 그렇지 않으면 은폐된 채 남을 수 있는 잠재적 사기, 절도 또는 기타 부정행위를 감지할 수 있도록 하기 위한 것입니다. 이 정책은 민감한 직책을 맡은 인력의 의무 휴가와 관련하여 미국 연방준비제도이사회가 제시한 감독상 기대 기준에 부합합니다.

민감한 데이터에 액세스할 수 있고 Citi에서의 직무 책임상 ‘민감’ 인력으로 지정된 모든 공급업체 인력은 MA 정책의 요건을 준수해야 합니다. 민감 인력은 매년 모든 정책 규칙 및 제한 사항에 따라 의무 휴가 기간을 계획하고 이를 완전히 이행해야 합니다. 이 기간 동안 민감 인력은 민감한 활동을 수행, 지시, 승인 또는 결재해서는 안 되며, 문의를 담당자에게 전달하는 경우를 제외하고 고객과의 상호 작용을 포함한 어떠한 연락에도 실질적인 답변을 해서는 안 됩니다. 의무 휴가 기간이 시작된 후 중단해야 하는 경우, 관리자 또는 Citi 비즈니스 담당자는 시스템 액세스를 복원할 수 있도록 컴플라이언스 시스템에서 해당 기간을 취소해야 하며, 이후 근로자는 새로운 의무 휴가 기간을 다시 계획해야 합니다.

부록 - 정의

에어 갭(Air-Gap)은 컴퓨터, 시스템 또는 네트워크를 다른 컴퓨터, 시스템 또는 네트워크와 물리적으로 분리하는 보안 조치입니다. 에어 갭 데이터 백업 아키텍처는 사이버 공격에 대한 노출을 제한하고 공격이 시작되기 전 시점으로 데이터를 복원할 수 있게 합니다.

준거법(관련 법률)에는 다음이 포함됩니다. (a) 주정부의 재산 압류 법률 및 규정, (b) 다양한 미국 연방기관이 발행한 규칙, 지침 및 기타 지침, 여기에는 2003년 미국 저축기관감독청이 시행한 공정·정확한 신용거래법의 114 조(때로는 Red Flag 지침 및 규정이라고도 칭함)가 포함됩니다.

가용 영역(Availability Zone)은 클라우드 서비스 공급업체가 로지컬 데이터 센터 그룹을 보유한 지점을 말합니다. 가용 영역이라 함은 클라우드 리전에서 전원, 네트워킹, 통신을 복제하는 이상의 개별 데이터 센터를 말합니다.

인공 지능(AI)은 컴퓨터 프로그램을 통해 인간의 지능을 모방하여 고전적인 통계적, 수학적, 계량경제학적 또는 재무적 접근 방식을 뛰어넘는 방식으로 추정, 예측, 권장 사항 또는 결정을 내리는 양적 방법, 시스템 또는 접근 방식('기술')을 말합니다. 여기에는 아래에 명시된 모든 AI 카테고리 및 생성형 AI, 에이전트형 AI, 대규모 언어 모델, 범용 AI(GPAI) 모델 등의 AI 변형이 포함됩니다.

AI 카테고리에는 다음이 포함됩니다.

- **정적 AI:** 오프라인에서 수동으로 훈련된 AI 기술이나 매개변수를 명시적으로 프로그래밍하여, 이를 추정, 예측, 권장 사항, 의사결정에 사용하는 AI 기술.
- **동적 AI:** "정적 AI"와 달리 프로덕션 환경에서 주기적으로 매개변수를 자동으로 재교육할 수 있는 기술.
- **자동 AI:** 기본 구조(예: 하이퍼파라미터, 입력 변수)를 자동으로 변경할 수 있는 "동적 AI" 기술.
- **인지 AI:** 특별히 훈련되지 않은 사안에 대해서도 자율적으로 결정하고 그러한 결정을 실행할 수 있는 기술.

머신 러닝(ML)은 모든 매개변수 표현이나 컴퓨터 작업 단계를 명시적으로 프로그래밍하지 않고, 데이터에서 표현이나 추론을 유도하는 AI의 하위 집합을 말합니다(예: 랜덤 포레스트, 신경망 기반 접근법). 이와 대조적으로, ML 하위 집합에 속하지 않는 AI 기술에는 퍼지 논리, 자연어 처리를 위한 복잡한 종속성 구문 분석 기술과 같은 기술이 포함됩니다.

사업활동소유주(Business Activity Owner, BAO)는 공급업체 관계에 관련된 특정 활동을 수행하고 능동적으로 관리하는 업무를 담당하는 Citi 직원입니다.

비즈니스 중개인(Business Introducer)은 Citi를 대신하여 신규 비즈니스 기회를 발굴하거나 기존 고객 관계를 관리하는 역할을 하는 공급업체입니다.

사업상 선물(Business Gift)은 Citi의 업무 또는 외부 당사자의 업무와 관련하여 Citi 직원이 주거나 수령한 가치 있는 물품(사업 접대 외에)으로 통상적으로 미화 25불 이하의 물품은 제외됩니다.

Citi 정보(Citi Information)는 Citi가 정보를 디지털·비디지털 형식으로 저장, 처리, 전송 또는 폐기하는 동안 Citi가 소유하거나 보호할 의무가 있는 정보입니다.

Citi 정보 분류에는 다음이 포함됩니다.

기밀(Confidential)은 개인을 언급하지 않고 높은 수준의 보호가 필요한 Citi 사업 및/또는 관련 당사자에 대한 정보입니다. 이 정보의 기밀성, 무결성 또는 가용성이 손상되면 Citi의 운영, 재무 상태, 프랜차이즈 또는 기업 고객에게 심각한 영향을 미칠 수 있습니다.

기밀 개인 식별 가능 정보(Confidential Personally Identifiable Information)는 해당 개인을 대상으로 한 신용 도용, 신용 사기 또는 기타 금융 사기 등의 불법 활동을 용이하게 할 가능성이 있는 개인에 대한 개인 정보입니다. 이 정보의 기밀성, 무결성 또는 가용성이 손상되면 재정적 손실이나 사기 등 개인에게 중대한 영향을 미칠 수 있습니다.

- 다른 개인 데이터와 결합되어 기밀 PII를 구성하는 개인 데이터 요소에는 개인 이름 또는 연락처 정보(주소, 전화번호 또는 이메일 주소)와 다음이 포함됩니다.
 - 자금 이동을 초래하거나 신용 도용 또는 사기를 저지르는 데 사용될 수 있는 거래 데이터 요소:
 - 신용/직불 카드 번호
 - 카드 검증 값(CVV) 또는 PIN
 - 신용 보고서 데이터(신용 점수)
 - 생년월일
 - 근로자 성과(평가/피드백) 또는 보상 정보
 - CCTV와 ATM 기록을 포함한 비디오 기록
- 특정 개인 데이터 요소는 단독으로 기밀 PII 를 구성해야 합니다.
 - 미국 사회보장번호, 정부에서 발행한 식별번호(사용상 및/또는 법적 보호 상태가 미국 사회보장번호와 동일함), 여권 번호, 운전면허증 번호 또는 개인의 세금 ID 번호

내부 정보(Internal)는 개인에 대한 정보가 아니며, 사업 목적으로 사용되며 중간 수준의 보호가 필요합니다. 이 정보의 기밀성, 무결성 또는 가용성이 손상되면 팀 또는 작업 그룹에 **제한적인 영향**을 미칠 수 있습니다.

- **개인 식별가능 정보(PII, Personally Identifiable Information):**
 - 개인 또는 가구를 식별하거나 식별하는 데 사용될 수 있음(예: 이름, 서명, 주소, 사회보장번호, 주민등록번호와 같은 고유 국가 식별자, 생년월일, 운전 면허증 번호),
 - 특정 개인·가구와 관련이 있거나, 그러한 개인이나 가구를 설명하는 내용이거나, 이와 연관되어 있거나, 합리적으로 연관할 수 있는 내용의 정보,
 - 개인 신용 인증 또는 특정 계정 액세스 제공 시 사용할 수 있는 정보(예:
 - 사용자 이름, 이메일 주소, 비밀번호, PIN, ID 번호, 보안 질문 답변), 또는 개인과 관련이 있고 민감한 정보(예: 개인 의료 정보나 건강 정보, 계좌 번호, 계좌 금액).
 - 개인정보에는 법에 의해 보호받는 의료 정보(미국 건강 보험 정보의 이전 및 그 책임에 관한 법률에서 정의된 대로), 민감한 개인정보 및 신용 정보(다양한 데이터 보호법/개인정보 보호 및 은행기밀 법에 정의됨)도 포함됩니다.

공개(Public)는 Citi 외부에서 자유롭게 접할 수 있거나, Citi 보도 자료 또는 Citi 에 관한 뉴스에서 보이는 기사와 같이 공개 사용할 수 있도록 의도된 정보를 의미합니다.

대외비(Restricted)는 특정 개인이나 그룹에서만 사용이 제한된 정보이며, Citi 또는 그 계열사에게 가장 민감한 정보로 가장 높은 수준의 보호가 필요합니다. 이 정보의 기밀성, 무결성 또는 가용성이 손상되면 Citi의 운영, 재무 상태, 프랜차이즈 또는 기업 고객에게 **심각한(전사적, 여러 지역, 여러 부문) 영향**을 미칠 수 있습니다.

- **민감한 PII(Sensitive PII)** 특정 법률에 의해 추가 보호가 필요하다고 명시된 개인 정보로, 불법적으로 차별하는 데 사용될 수 있거나 개인에게 부당함이나 해를 끼칠 수 있는 정보입니다. 이 정보의 기밀성, 무결성 또는 가용성이 손상되면 개인에게 상당한 영향(재정적 손실, 사기 또는 차별적 영향을 포함하되 이에 국한되지 않음)을 미칠 수 있습니다.
- 구체적으로 다음과 관련된 데이터: 인종, 종교, 종교적이거나 철학적 신념, 민족성, 정치적 성향 또는 의견, 조합원 신분, 범죄 배경 정보 또는 범죄, 유전자 데이터, 생체 정보 또는 개인의 성적 성향 또는 활동.
 - 개인의 의료 기록 또는 정신 또는 신체적 상태에 대한 정보를 포함하는 개인 건강 정보(PHI).

고객(Client)은 Citi 의 모든 고객을 의미하며 개인(즉 자연인), 사업체, 기관, 조직 및 법인을 포괄합니다.

클라우드 리전(Cloud Region)은 클라우드 서비스 공급업체가 데이터 센터(들)를 클러스터링하는 물리적 위치입니다.

통신 장비, 시스템 및 서비스(Communications Equipment, Systems and Services)는 서면, 음성, 비디오 전자 통신을 전송하는 데 사용되는 하드웨어, 소프트웨어나 애플리케이션입니다. eComm 채널에는 다음이 포함되지만 이에 국한되지는 않습니다. 컴퓨터, 랩톱, 태블릿, 모바일 기기나 휴대폰, 여기에는 "개인 기기 사용"(BYOD), 블랙베리, 전화기, 팩스(팩스 서비스), 인트라넷 및 인터넷 액세스, Wi-Fi 서비스, 이메일 서비스, Microsoft Lync, Skype 및 Bloomberg 메시지와 같은 인스턴트 메시징 서비스, 통신 기능이 임베드된 웹사이트 및 애플리케이션, Zoom 또는 Microsoft Teams 와 같은 화상 회의 플랫폼이나 협업 플랫폼, 그리고 각종 소셜 미디어 서비스, 대화형 정보 공유 서비스, 제삼자 대화방, 전자 게시판 및 블로그.

콘텐츠(Content)는 (a) Citi 나 그 대리인이나, Citi 계열사나 그 대리인이 공급업체에 직간접적으로 제공하거나 공급업체가 사용할 수 있게 하거나, (b) 해당 서비스를 통해 생성, 제작되거나 (c) 전술한 내용에서 파생된 Citi 의 기밀 정보 및 기타 모든 데이터, 보고서, 통계 또는 모든 유형의 정보를 의미합니다.

계약(Contract)은 제안, 수락, 고려, 당사자들의 의무 및 목적의 적법성을 포함하는 둘 이상의 당사자가 서명한 법적 문서입니다. 계약의 예에는 제품 및 서비스에 대한 마스터 약정, 작업 명세서 / 작업 지시서, 개정 및 부록, 스케줄, 명령 또는 Citi 실체 및 공급업체가 서명한 일체의 다른 문서가 포함됩니다. 기밀유지약정(NDA) 또한 본 기준서의 목적상 계약으로 간주됩니다.

접속 거부(Denial of Access, DOA) 테스트는 정해진 RTO 안에 복구될 수 있는 Citi 의 업무 절차에 대한 공급업체의 인력 및 지원을 검증합니다.

서비스 거부(Denial of Service, DOS) 테스트는 Citi 비즈니스를 지원하는 공급업체의 애플리케이션 및 기본 인프라 구성 요소를 정의된 복구 목표 시간(RTO) 내에 복구할 수 있는지 검증합니다.

"예치 자료(Deposit Materials)"는 다음 하위 섹션(i)-(vi)를 의미하며, 해당되는 경우 Citi 환경 내에서 작동하도록 Citi 에 라이선스가 부여된 소프트웨어 또는 Citi 에 제공된 호스팅 서비스에 대해 공급업체가 사용하는 자료를 통칭하여 의미합니다.

- (i) Citi 와 체결한 해당 계약에 명시된 라이선스 소프트웨어 또는 호스팅 서비스의 개발, 운영, 유지보수 및 지원에 사용되는 소스 코드의 정확한 복제본(및 해당 소프트웨어 또는 호스팅 서비스의 모든 이후 버전), 그리고 해당 소프트웨어에 대한 모든 문서(일부 소스 코드 사본을 Citi 가 이미 보유하고 있는지 여부와 관계없이)("소스 코드 예치");
- (ii) 공급업체가 라이선스 소프트웨어 또는 호스팅 서비스의 개발, 운영, 유지관리 및 지원과 관련하여 권리를 보유한 제 3 자 소프트웨어의 소스 코드;
- (iii) 소프트웨어 또는 호스팅 서비스를 운영, 유지보수 및 지원하는 데 필요한, 예치 자료에 포함된 소스 코드를 실행 가능한 형태로 변환하는 데 필요한 디버거, 어셈블러, 컴파일러 등의 모든 소프트웨어 도구의 라이선스 사본;
- (iv) 위에 이미 제공되지 않은 범위 내에서, 다음 사항을 제공하는 모든 문서: (A) 예치 자료의 일반적인 설명 및 운영; (B) 아키텍처 및 기본 프로그램 기능; (C) 데이터 흐름 정보; (D) 상세한 메모리 맵 및 목록; (E) 입력/출력 포트 맵; (F) 해당 프로그래밍 언어의 일반적인 기술 프로그래머가 예치 자료에 포함된 소스 코드를 사용하고 수정할 수 있도록 하는 기타 세부 정보;
- (v) 소프트웨어 또는 호스팅 서비스와 관련하여 Citi 또는 Citi 를 대신하는 적격한 제 3 자가 소프트웨어 또는 호스팅 서비스를 사용, 운영, 수정 및 향상시키는 데 합리적으로 필요한 모든 기타 기술 정보;
- (vi) 소프트웨어 또는 호스팅 서비스와 관련하여 사용되는 모든 제 3 자 소프트웨어 및 기술 목록(소프트웨어에서의 사용에 대한 합리적인 세부 정보 및 해당 소프트웨어나 기술 제공자의 연락처 정보 포함). Citi 는 예치 자료에 하위 섹션(ii)에 명시된 것 이외의 제 3 자의 소스 코드가 포함되어 있지 않음을 인정하고 이에 동의합니다. 그리고
- (vii) 호스팅 서비스 관련:
 - a. 클라우드 호스팅된 운영 환경의 축소판 복제본 또는 환경별 클라우드 관련 자료와, Citi 의 운영 환경을 복제하는 데 필요한 기타 정보(다음을 포함하되 이에 국한되지 않음): 코드, 테라폼 스크립트, 클라우드 리소스, 클라우드 포메이션 템플릿, 구성 파일, 클라우드 테넌트, 클라우드 구독, 머신 이미지, Docker 이미지 및 소프트웨어의 소스 코드로서의 인프라와 같은 인프라. 그리고,
 - b. 소프트웨어 내에 보관된 Citi 의 데이터 사본.

전자 통신(Electronic Communications)은 유선·무선 신호를 통해 직원이 전자적 수단으로 전송, 수신 또는 사용하는 메시지나 정보를 말합니다. 전자 통신에는 문자 메시지, 이메일, P2P 또는 인스턴트 메시지, 블로그 게시물, 소셜 미디어 게시물, WhatsApp, WeChat, Line, Signal 또는 Viber 와 같은 메시징 애플리케이션을 통해 전송된 메시지 등이 포함되지만 이에 국한되지 않으며, 첨부 파일, 스크린샷, 녹음된 음성 또는 비디오 파일, 실시간 음성 또는 영상, 그리고 전자 통신 장비, 시스템 및 서비스를 통해 생성, 수신, 다운로드, 저장, 전송, 삭제 또는 사용된 파일이 포함됩니다.

기능 ID(Functional ID)는 ADMIN 또는 ROOT 와 같은 일반 ID 로 사람이나 프로세스가 보안 시스템에 액세스하는 데 사용됩니다. ID 및 액세스 관리(IAM) 운영의 핵심은 Citi 가 기능 ID 사용과 관련된 리스크로부터 보호하기 위한 구체적이고 명확한 통제 기능을 갖추도록 보장하는 것입니다.

프랜차이즈 크리티컬 프로세스/프랜차이즈 크리티컬 애플리케이션(Franchise Critical Processes / Franchise Critical Applications, FCA)은 Citi 가 프랜차이즈 크리티컬 비즈니스 기능을 성공적으로 실행하는 데 필수적인 요소로 식별한 프로세스/애플리케이션을 말합니다.

사기(Fraud)는 다른 사람을 속일 목적으로 설계된 행위, 허위 진술 또는 누락을 의미하며, 피해자가 손실을 입거나 가해자가 이익을 얻는 결과로 이어집니다.

호스팅 서비스에는 호스팅 서비스, 모든 애플리케이션 및 기타 소프트웨어, 데이터베이스, 웹사이트, 서버, 하드웨어, 네트워크, 통신 및 기타 장비, 그리고 호스팅 서비스 환경에 설치되거나 그 안에서 사용되는 기타 기술을 제공하기 위해 공급업체가 설치한 애플리케이션, 공급업체가 관리하거나 활용하는 모든 시설 및 환경, 그리고 모든 각각의 업데이트와 지원 서비스가 포함됩니다(단 모든 콘텐츠와 Citi 시스템은 제외됨).

신원 확인 데이터(Identity Verification Data, IVD)는 보안 질문(SQ) 또는 지식 기반 인증(KBA) 질문으로 정의됩니다. 보안 질문은 일반적으로 애플리케이션에서 정의하고 최종 사용자가 답변합니다. 예로는 어머니의 성, 출생지, 좋아하는 아이스크림 등이 있습니다. 두 가지 유형의 질문 모두 인증 데이터로 처리해야 합니다.

정보 보안(Information Security), 즉 "IS"는 컴퓨터나 컴퓨터 시스템을 무단 액세스나 공격으로부터 보호되는 상태를 의미하며, 이러한 상태로 인해 (a) 컴퓨터나 컴퓨터 시스템이 계속 사용 가능하고 작동하며, (b) 컴퓨터나 또는 컴퓨터 시스템의 무결성이 유지되고, (c) 컴퓨터나 컴퓨터 시스템에(서) 저장되거나, 처리되거나 전송되는 정보의 무결성과 기밀성이 유지됩니다.

IS 위협(IS Threat)은 컴퓨터 또는 컴퓨터 시스템에서 수행되거나 그를 통해 이루어진 행위나 활동(알려진 것이든 의심되는 것이든 관계없이)으로서, 해당 컴퓨터나 다른 컴퓨터 또는 컴퓨터 시스템의 IS 에 해를 끼치거나 부정적인 영향을 미칠 수 있는 것을 의미합니다.

IS 취약점(IS Vulnerability)은 하나 이상의 IS 위협에 의해 악용될 수 있는 컴퓨터 또는 컴퓨터 시스템의 모든 취약점을 의미합니다.

비고객/비수익 창출(Non-Client / Non-Revenue Generating)은 법률, 감독, 규제 및 비즈니스 연속성 활동을 포함하여 수익 창출 활동과 관련되지 않은 비즈니스에 중요한 활동으로 정의됩니다.

기밀유지협약서(NDA)는 Citi와 공급업체 간의 약정으로서 정보의 교환, 이용 및 공개가 본 약정의 조항에 따라 지배됩니다.

오픈 소스 소프트웨어는 소스 코드 또는 컴파일된 컴퓨터 프로그램을 의미하며, 소스 코드는 일반 대중이 사용하거나 원래 설계에서 수정할 수 있도록 공개되어 있습니다.

인사: 직접적으로 명시했던 맥락에서 도출했든, 공급업체와 그 계열사, 이사, 임원, 직원, 대리인, 감사원, 컨설턴트, 서비스 제공자 및 계약자(Citi 직원 제외)를 의미합니다. 공급업체 인력에는 하청업체의 이사, 임원, 직원, 대리인, 감사원, 컨설턴트 또는 기타 대표도 포함됩니다."

기록 목록(Records Inventory)은 Citi 기록의 기록 유형, 위치, 일자 등등을 포함하는 상세 목록으로서 사업체가 전체 정보 주기 동안 기록을 적절히 관리하는데 필요합니다.

정보 보류(Information Hold)는 기록 및 정보에 부과되는 요건으로, 보류를 발령한 기관이 이를 해제할 때까지 해당 기록 및 정보의 수정 또는 폐기를 유예하는 것을 말합니다.

복구 역량(Recovery Capacity)은 공급업체의 제품 및 서비스의 양, 수량 또는 제공 속도를 의미하며, 이는 일반적인 제품 및 서비스 제공량 대비 백분율로 표현됩니다.

복구 기간(Recovery Duration)은 공급업체가 복구 모드에 있는 동안 운영을 유지할 수 있는 최대 기간(달력일 기준)입니다.

복구 지점 목표(Recovery Point Objective)는 업무 중단 발생 후 복구되어야 하는 데이터의 과거 시점을 시간(시간 단위)으로 나타낸 것입니다. 이는 중대한 사고로 인해 IT 서비스에서 데이터가 손실될 수 있는 최대 목표 기간입니다. RPO는 IT 서비스에 영향을 미치는 주요 사고가 발생했을 때 데이터가 손실될 수 있는 최대 기간을 측정한 것입니다. 이것은 데이터 손실량에 대한 직접적인 측정치는 아닙니다. (예: 이전 날 처리의 종료 시까지)

복구 시간 목표(Recovery Time Objective)는 서비스 차질로부터 제품 및 서비스의 복원까지의 소요 시간을 말합니다.

"공개 사유"는 다음 중 하나 이상을 의미합니다.

- (i) 공급업체(A)가 지불 불능이 되거나 일반적으로 만기가 되는 채무를 지불할 능력이 없음을 인정한 경우, (B) 자발적이든 비자발적이든, 국내외 파산 또는 지급불능 관련 법률에 따른 절차의 대상이 된 경우로서, 해당 절차가 7 영업일 이내에 전면 중지(stay)되지 않거나, 제출일로부터 45 일 이내에 기각되거나 무효화되지 않은 경우, (C) 채권자에게 유리하도록 일반적인 양도를 수행하는 경우, 또는 (D) 관할 법원의 명령에 따라 수탁자, 재산관리인, 보관인 또는 유사한 대리인이 지정되어 그 자산이나 사업의 상당 부분을 관리하거나 처분하게 되는 경우.

자원관리조직(Resource Management Organization, RMO)은 Citi의 글로벌 엔드 투 엔드 자원 관리를 담당합니다. 여기에는 전략적 소싱, 구매 지불 업무, 인력 관리 부서, 공급업체 관리 프레임워크 등이 포함됩니다.

RMO 소싱 매니저(Sourcing Manager)는 자원관리조직(RMO)에 속한 직원으로서 RFP 및 다른 공급업체 선정 활동, 계약 조건의 관리 및 재무적 평가 승인 요건을 포함한 계약 업무 조건, 요건 및 가격 책정 협상을 담당하는 직원입니다.

개인에 대한 **심각하거나 치명적인 악영향**은 그 영향이 개인에게 합리적으로 상당한 악영향을 초래할 수 있다는 것을 의미하며, 여기에는 재정적 손실이나 실직 및 구직의 어려움, 인권 손실 개인적 또는 대중적 수치심이나 부적절한 구속 등이 포함됩니다.

하청업체: 하청업체는 제 3 자가 Citi와 계약한 서비스나 활동의 일부 또는 전부를 수행하기 위해 고용한 제 4 자(개인 또는 단체)를 말합니다.

안내:

질문 1: 제 3 자 하청업체를 모두 보고해야 합니까?

답변 1: 현재 수행 중인 서비스와 관련된 하청업체만 보고하면 됩니다. 하청업체가 수행하는 서비스 또는 활동의 예는 다음과 같지만 이에 국한되지 않습니다.

*Citi가 제 3 자와 계약한 서비스/활동을 직접 또는 간접적으로 지원하는 기술 또는 소프트웨어 서비스를 수행하는 하청업체 또는

*Citi 기밀 또는 그 이상의 정보에 대한 접근을 포함하는 서비스를 제공하는 하청업체 또는

*기존/잠재적 Citi 고객과 직접 또는 간접적으로 상호 작용하는 하청업체 또는

*관계자 동행 없이 Citi 건물 내외부에서 Citi 문서의 파쇄 서비스나 보관 서비스를 수행하는 하청업체, 또는

*지불, 징수, 대출 등 핵심적인 은행 업무 기능이나 서비스를 지원하는 하청업체

공급업체: 이 'Citi의 공급업체 요건' 문서에서 "공급업체"란, Citi 법인과 직접 상품 또는 서비스를 제공하거나, Citi 법인의 비즈니스 목표 달성을 지원하기 위해 비즈니스 계약을 체결한 외부 제 3 자를 의미합니다. 외부 제 3 자는 Citi 가 아닌 단체로 정의됩니다. 공급업체는 Citi 법인의 클라이언트 또는 고객일 수도 있고 Citi 클라이언트 및 고객과의 상호 작용을 지원할 수도 있습니다. 그러나 단순히 Citi 의 고객 또는 클라이언트라는 이유만으로 체결된 계약은 본 문서의 범위 내에서 공급업체 관계로 간주되지 않습니다.

임시 정보: 기록은 Citi 가 법적, 규제적, 또는 승인된 사업상의 이유로 반드시 유지 관리할 의무가 있는 정보의 최종적이고 가장 완전한 버전입니다. 다른 모든 정보는 '임시 정보'로 분류됩니다.