아래 번역은 단지 정보 제공 목적으로 제공됩니다. 이 번역본과 영문본 간에 차이, 불일치 또는 상충이 있는 경우(번역 지연 포함), 최종 업데이트된 영문본이 우선합니다.

Amazon 벤더 보안 정책

최종 업데이트: 2024 년 9 월 11 일

1. **범위.** 공급업체는 이러한 보안 요건(이하 "보안 정책")을 준수해야 합니다. 이 보안 정책은 공급업체의 다른 계약상 또는 법적 의무를 제한하지 않습니다. 이 보안 정책과 공급업체와 Amazon 이 체결한 다른 계약이 상충하는 경우, 공급업체는 Amazon 정보를 더 엄격하게 보호할 수 있는 제한적인 요건을 준수해야 합니다.

2. **업데이트.**

2.1 Amazon 은 수시로 이 보안 정책을 상업적으로 합당하게 업데이트할 수 있으며, 이는 보안 정책의 "최종 업데이트" 날짜로부터 30 일 후에 효력이 발생합니다. 공급업체는 업데이트가 발효되면 업데이트된 보안 정책을 준수해야 합니다.

2.2 공급업체가 이러한 업데이트가 발효되기 전에 사전 알림을 받고자 하는 경우 본 보안 정책 웹페이지에 제공된 구독 양식을 사용하여 업데이트 알림 수신을 신청할 수 있습니다. 공급업체는 업데이트 알림 수신을 위해 제공한 모든 공급업체 연락처 정보를 항상 최신 상태로 정확하게 유지해야 합니다. 공급업체에서 실제로 업데이트 알림을 받았는지 여부에 관계없이 이메일을 통해 전송된 경우 업데이트 알림을 수신한 것으로 간주합니다.

3. **허용된 목적.**

3.1 **명시적 승인**. 공급업체는 계약에 따라 명시적으로 승인된 Amazon 정보만 계약에 명시된 제품 또는 서비스를 제공하기 위한 목적(이하 "허용된 목적")으로만 처리할 수 있습니다.

3.2 **데이터 보관**. 공급업체는 허용된 목적으로 필요한 기간 동안만 Amazon 정보를 보관합니다.

3.3 **명시적 제한**. 공급업체는 익명 처리된 경우에도 (a) Amazon 정보를 처리하거나 (b) Amazon 정보를 양도, 대여, 물물 교환, 거래, 판매, 임대 또는 제 3 자에게 배포 또는 제공하거나 (c) Amazon 정보를 사용하여 인공지능(AI) 또는 머신러닝(ML) 모델을 개발, 훈련 또는 개선하는 행위를 해서는 안 됩니다.

4. **최소 보안 요건**. 공급업체는 업계 모범 사례(국제표준화기구("ISO") 표준 27001 및 27002, 미국표준기술연구소("NIST") 사이버보안 프레임워크 또는 기타 유사 표준 포함)에 따라 물리적, 관리적, 기술적 안전 조치를 취해야 합니다. 공급업체에서 취해야 하는 안전 조치에는 아래 4.1 항 ~ 4.18 항에 설명된 최소 요건도 포함됩니다.

4.1 **서면 정보 보안 프로그램**. 공급업체는 서면으로 작성된 정보 보안 프로그램을 시행해야 하며, 여기에는 (a) 이 보안 정책에 명시된 요건을 충족하는 적절한 정책, 절차 및 표준을 포함하고, (b) 보안 문제(보안 사고 포함)를 관리하고 이에 대해 소통할 수 있는 보안 담당자를 지정하고, (c) 최소 연 1 회 이상 검토하고 필요 시 업데이트하며, (d) 직원에게 적용해야 합니다. 공급업체는 정보 보안 프로그램을 모니터링 및 시행하고 위반 사항을 해결해야 합니다.

4.2 **패치 관리**. 공급업체는 최신 업그레이드, 업데이트, 버그 수정 및 새 버전으로 대상 정보 시스템을 최신 상태로 유지합니다. 공급업체는 패치할 수 없는 자산에 대해 완화 조치를 마련해야 합니다.

4.3 **로그 기록**. 공급업체는 (a) 허용된 목적을 위해 공급업체에 제공된 Amazon 계정 또는 자격 증명의 모든 사용(승인 및 비승인 포함)에 대한 로그 데이터, (b) Amazon 직원 또는 정보 또는 대상 정보 시스템에 액세스할 수 있는 직원을 사칭하거나 이를 시도한 사례에 대한 로그 데이터를 포함하여 감사, 이벤트 및 보안 로그를 수집 및 관리하고 보관합니다. 이러한 로그에는 (i) 이벤트를 시작한 직원 또는 계정, (ii) 이벤트 시간, (iii) 영향을 받은 시스템, 데이터 또는 기타 리소스 등 기록된 각 이벤트에 대해 알 수 있는 충분한 데이터가 포함되어 있어야 합니다. 공급업체는 무단 활동을 감지, 조사하고 복구할 수 있도록 이러한 로그를 정기적으로 분석해야 합니다.

아래 번역은 단지 정보 제공 목적으로 제공됩니다. 이 번역본과 영문본 간에 차이, 불일치 또는 상충이 있는 경우(번역 지연 포함), 최종 업데이트된 영문본이 우선합니다.

4.4 멀웨어 방어. 공급업체는 (a) 모든 대상 정보 시스템에 멀웨어 방지 소프트웨어 또는 동등한 보안 제어를 배포하고, (b) 멀웨어 방지 소프트웨어 또는 동등한 보안 제어의 업데이트, 서명 및 구성을 유지하고, (c) 악성 또는 무단 코드의 설치, 확산 및 실행을 감지, 방지 및 시정하는 시스템을 구성해야 합니다.

4.5 위험 관리 프로그램. 공급업체는 위험 분석, 위험 처리, 위험 수용 및 예외에 대한 절차를 규정한 서면 정보 보안 위험 관리 프로그램을 갖추어야 합니다.

4.6 보안 인식 교육. 공급업체는 채용 시 및 그 이후 최소 연 1 회 이상 직원들을 대상으로 정보 보안 및 데이터 개인정보 보호에 대한 교육을 실시해야 합니다. 공급업체는 또한 직원들에게 보안 및 데이터 개인정보 처리방침에 대한 업데이트를 제때 알려야 합니다.

4.7 데이터 인벤토리. 공급업체는 (a) 처리하는 Amazon 정보, (b) Amazon 정보를 처리하는 방법 및 장소(예: 최신 아키텍처 다이어그램)에 관한 정보를 문서화하고 유지해야 하며, Amazon 에서 요청 시 이를 제공해야 합니다.

4.8 보안 테스트.

4.8.1 공급업체는 본 보안 정책의 요건을 충족하는지 확인하기 위해 연례 테스트를 수행합니다.

4.8.2 공급업체는 자사의 보안 방어에 대한 침투 테스트를 최소 연 1 회 이상 진행해야 합니다. 침투 테스트에는 (a) 공급업체 네트워크 내부 및 외부에서 테스트, (b) 소셜 엔지니어링(예: 피싱 시뮬레이션), (c) 무선 네트워크에 대한 보안 테스트도 포함되며, 공급업체는 취약성 관리 프로그램을 통해 확인된 취약성을 해결해야 합니다. Amazon 에서 요청 시, 공급업체는 침투 테스트 및 취약성 시정 결과를 제공합니다.

4.9 네트워크 보안. 공급업체는 특히 외부 네트워크로부터의 무단 네트워크 액세스를 제한하여 대상 정보 시스템을 보호해야 합니다. 무단 액세스로부터 시스템을 보호하기 위해 방화벽 또는 기타 동등한 보안 제어를 유지 및 구성하고, 방화벽 규칙 세트를 최소 연 1 회 이상 검토하여 모든 규칙이 유효하고 문서화된 비즈니스 사례가 있는지 확인해야 합니다.

4.10 적합한 환경. 공급업체는 목적에 적합한 환경에서만 Amazon 정보를 처리하고 계약에 따라 허용된 경우를 제외하고 테스트 환경에서 Amazon 정보를 처리해서는 안 됩니다.

4.11 암호화. 공급업체는 업계 모범 사례에 따라 보관 중이거나 외부 네트워크에서 전송되는 모든 Amazon 정보를 암호화해야 합니다. 공급업체 내부 네트워크에서 Amazon 정보를 전송하는 경우, 업계 모범 사례에 부합하는 암호화된 프로토콜을 통해 전송해야 합니다. 공급업체는 업계 모범 사례에 따라 암호화 키를 관리하고 보호해야 합니다.

4.12 관리 권한의 통제된 사용. 공급업체는 NIST 사이버 보안 프레임워크 또는 ISO 27002 에 따라 관리 기능을 관리하고, 최소한 관리 계정을 표준 계정과 분리하고 관리 계정을 관리 기능 수행에 필요한 기능으로만 제한합니다. 공급업체는 모든 관리 계정 활동을 개별 사용자별로 기록하고, 표준 계정에 제공되는 관리 기능은 최소 권한을 기준으로 개별 사용자별로 기록합니다.

4.13 액세스 통제.

4.13.1 **고유 ID**. 공급업체는 관리 액세스 권한이 있는 계정을 포함하여 Amazon 정보 또는 대상 정보 시스템에 액세스할 수 있는 직원에게 개별 고유 ID 를 할당해야 합니다.

4.13.2 **"알아야 할 필요"가 있는 경우로 제한**. 공급업체는 Amazon 정보 및 대상 정보 시스템에 대한 액세스를 허용된 목적상 "알아야 할 필요"가 있는 직원으로 제한합니다.

아래 번역은 단지 정보 제공 목적으로 제공됩니다. 이 번역본과 영문본 간에 차이, 불일치 또는 상충이 있는 경우(번역 지연 포함), 최종 업데이트된 영문본이 우선합니다.

4.13.3 **사용자 액세스 검토**. 공급업체는 최소 90 일마다 Amazon 정보 및 대상 정보 시스템에 액세스할 수 있는 직원 및 서비스 목록을 검토하고 더 이상 필요하지 않은 계정에서 액세스 권한을 삭제합니다.

4.13.4 **통합 인증(SSO)**. Amazon 직원 인증이 필요한 모든 공급업체 서비스는 인증을 위해 Amazon ID 제공업체(예: Amazon Federate)와 통합해야 합니다. 이러한 서비스의 경우 공급업체가 제공하거나 공급업체가 관리하는 자격 증명을 인증에 사용해서는 안 됩니다.

4.14 **암호 관리.**

4.14.1 **강력한 암호.** 공급업체는 대상 정보 시스템에서 시스템 암호 및 기타 보안 매개변수에 대해 제조업체에서 제공한 기본 설정을 사용해서는 안 됩니다. 모든 대상 정보 시스템에서 NIST SP 800-63B 에 설명된 모범 사례에 따라 시스템에서 시행하는 "강력한 암호" 사용을 의무화하고 이를 확인해야 합니다. 공급업체는 모든 암호와 액세스 자격 증명을 기밀로 유지하고 직원 간에 공유하지 않아야 합니다.

4.14.2 **잠금**. 공급업체는 계정에서 연속 10 회 이상 잘못된 암호를 시도하는 경우 Amazon 정보 또는 대상 정보 시스템에 액세스할 수 있는 계정을 비활성화하여 "계정 잠금"을 시행하고 유지해야 합니다.

4.15 **원격 접속, 다중 인증**. 공급업체는 원격으로 자사 공급업체 네트워크, 시스템, 애플리케이션 또는 기타 자산에 액세스할 때 다중 인증(즉, 사용자 인증 시 최소 2 가지 요소를 요구)을 적용해야 합니다.

4.16 **"대량" 액세스**. 본 조항의 목적상 "대량" 액세스는 데이터베이스 쿼리, 보고서 생성 또는 기타 데이터의 대량 전송을 통해 데이터에 접속하는 경우를 의미합니다.

4.16.1 계약에 명시적으로 규정되거나 Amazon 에서 서면으로 달리 정한 경우를 제외하고, 공급업체는 Amazon 정보가 Amazon 또는 공급업체에서 관리하는 데이터베이스에 있거나 파일 기반 아카이브(예: 플랫 파일)에 저장하는 등 기타 방법을 사용하여 저장된 Amazon 정보에 "대량"으로 액세스하거나 이를 허용해서는 안 됩니다.

4.16.2 Amazon 이 "대량" 액세스를 승인하는 경우, 공급업체는 (a) "알 필요가 있는" 특정 직원으로만 액세스를 제한하고, (b) 4.3 항에 명시된 요건에 따라 명시적인 승인을 받고 이를 로그에 기록해야 합니다. 10 항 보안 검토 또는 11 항 보안 사고와 관련하여 Amazon 에서 요청 시 공급업체는 본 조항에 언급된 모든 "대량" 액세스에 대한 로그 기록을 제공해야 합니다.

4.17 데이터 분리. 공급업체는 Amazon 정보를 공급업체 및 제 3 자 정보와 항상 물리적 또는 논리적으로 분리해야 합니다. 분리가 불가능한 경우, 공급업체는 로그 기록, 삭제 및 사고 대응 목적으로 Amazon 정보를 다른 정보와 구별할 수 있도록 해야 합니다.

4.18 **공급업체 직원 보안.**

4.18.1 공급업체는 Amazon 정보에 대한 액세스 권한이 부여된 직원이 기밀을 유지하고 허용된 목적으로만 정보를 사용할 수 있도록 모든 합리적인 예방 조치를 취해야 합니다. 이러한 예방 조치로는 비공개 계약을 체결하거나 공급업체 정책을 통해 기밀 유지 요건을 부과하는 방법 등이 있습니다.

4.18.2 직원이 (a) Amazon 정보에 더 이상 액세스할 필요가 없거나 (b) 더 이상 공급업체 직원으로서 자격이 없는 경우 공급업체는 24 시간 내에 Amazon 정보 및 대상 정보 시스템에 대한 액세스 권한을 해지해야 합니다. (a) 또는 (b) 중 하나가 발생한 후 24 시간이 지난 후에도 직원이 Amazon 정보 또는 대상 정보 시스템에 액세스 권한을 보유하고 있는 경우 공급업체는 이를 인지한 후 24 시간 이내에 security@amazon.com 으로 이메일을 보내 Amazon 에 알려야 합니다.

아래 번역은 단지 정보 제공 목적으로 제공됩니다. 이 번역본과 영문본 간에 차이, 불일치 또는 상충이 있는 경우(번역 지연 포함), 최종 업데이트된 영문본이 우선합니다.

5. **결제 보안 요건**. 공급업체가 결제 카드 소지자 데이터에 액세스할 수 있거나 이를 처리하는 경우 공급업체는 최신 버전의 결제 카드 업계 데이터 보안 표준(PCI DSS)을 준수해야 합니다.

6. **하청업체.**

6.1 공급업체는 Amazon 의 사전 서면 동의 없이 본 보안 정책에 따른 의무를 제 3 자(이하 "하청업체"로 총칭함)에게 하도급하거나 위임할 수 없습니다. 체결된 하도급 계약 또는 위임 계약 조건과 별개로 공급업체는 본 보안 정책에 따른 의무를 모두 이행해야 할 책임이 있습니다. 본 보안 정책의 약관은 공급업체의 하청업체 및 해당 하청업체 직원에게 구속력을 갖습니다.

6.2 공급업체에서 하청업체의 대상 정보 시스템을 사용하는 경우 공급업체는 해당 정보 시스템과 시행하고 있는 보안 제어에 대한 보안 검토를 수행하고, Amazon 에서 요청 시 하청업체의 대상 정보 시스템의 보안 제어에 관한 정기 보고서를 Amazon 에서 요청한 형식(예: 증명 업무를 위한 표준에 관한 성명서 제 16 호(SSAE 16))으로 제공합니다.

7. Amazon 관리 정보 시스템에 대한 액세스. Amazon 은 허용된 목적에 한하여 웹 포털 또는 기타 비공개 웹사이트 또는 엑스트라넷(이하 각각 "Amazon 관리 정보 시스템")을 통해 Amazon 정보를 처리할 수 있는 권한을 공급업체에 부여할 수 있습니다. Amazon 에서 공급업체에 Amazon 관리 정보 시스템을 사용하여 Amazon 정보를 처리하도록 허용하는 경우, 공급업체와 직원은 다음 요건을 준수해야 합니다.

7.1 **계정**. 공급업체는 직원만 Amazon 에서 각 개인에게 부여한 Amazon 관리 정보 시스템 계정을 사용하고 액세스 자격 증명을 기밀로 유지하고 공유하지 않도록 해야 합니다.

7.2 **시스템**. 공급업체와 직원은 (a) 공급업체가 관리하고 전체 디스크 암호화를 사용하는 운영 체제를 실행하며 (b) 4.2 항(패치 관리), 4.4 항(멀웨어 방어) 및 4.9 항(네트워크 보안)에 명시된 요건을 충족하는 전산 또는 처리 시스템, 애플리케이션을 통해서만 Amazon 관리 정보 시스템을 사용해야 합니다.

7.3 **제한 사항**. Amazon 에서 서면으로 사전 승인한 경우를 제외하고 공급업체와 직원은 Amazon 관리 정보 시스템에 있는 Amazon 정보를 여타 매체에 다운로드 또는 미러링하거나 영구적으로 저장할 수 없습니다.

7.4 **계정 해지**. (a) 더 이상 Amazon 관리 정보 시스템에 액세스할 필요가 없거나 (b) 더 이상 공급업체 직원 자격이 없는 경우(예: 해당 직원이 공급업체에서 퇴사하는 경우) 공급업체는 즉시(최대 24 시간 이내에) 해당 직원의 Amazon 관리 정보 시스템에 대한 액세스 권한을 해지하거나 Amazon 에 이를 알리고 액세스 권한을 삭제하도록 해야 합니다.

8. **Amazon 도메인 또는 URL.** 공급업체가 Amazon 이 단독으로 사용하도록 제공한 도메인 또는 URL 은 계약 종료 후 최소 5 년 동안 공급업체가 제 3 자에게 제공하거나 제 3 자가 재사용해서는 안 됩니다.

9. 데이터 반환 및 삭제, 매체 포렌식 파기

9.1 **데이터 반환 및 삭제**. Amazon 에서 요청 시 공급업체는 신속하게(72 시간 이내에) Amazon 에서 반환 및/또는 삭제를 요청하는 통지를 받은 후 그에 따라 모든 Amazon 정보를 Amazon 에 반환하고 안전하게 삭제해야 합니다. 또한 공급업체는 허용된 목적을 달성하거나 계약이 해지 또는 만료되는 시점 중 빠른 시점을 기준으로 30 일 이내에 Amazon 정보의 모든 라이브(온라인 또는 네트워크에서 액세스할 수 있는) 인스턴스를 영구적으로 안전하게 삭제합니다. Amazon 에서 요청하는 경우, 공급업체는 모든 Amazon 정보를 삭제했음을 서면으로 증명해야 하며, 명확성을 위해, 본 조항은 9.3 항에 따른 보관 사본에는 적용되지 않습니다.

9.2 **데이터 위생 처리**. 공급업체에서 삭제한 모든 Amazon 정보는 해당 기기 유형 제거에 관한 NIST SP 800-88 개정 1 판, 매체 위생 처리 지침(2014 년 12 월 18 일, 부록 A)에 명시된 최소 위생 처리 권장 사항에 따라 삭제해야 합니다. NIST SP 800-88 에 해당 기기 유형에 대한 지침이 없는 경우 공급업체는 (a) NIST SP 800-88 에 명시된 방법으로

아래 번역은 단지 정보 제공 목적으로 제공됩니다. 이 번역본과 영문본 간에 차이, 불일치 또는 상충이 있는 경우(번역 지연 포함), 최종 업데이트된 영문본이 우선합니다.

제거하거나 (b) NIST SP 800-88 에 명시된 방법으로 파기하거나 (c) Amazon 정보 분류 및 민감도에 따라 Amazon 에서 요구하는 기타 표준 중 한 가지 방식으로 Amazon 정보가 포함된 기기를 파기해야 합니다.

9.3 **보관 사본**. 공급업체에서 법에 따라 Amazon 정보의 보관 사본을 보관해야 하는 경우 공급업체는 보관된 Amazon 정보를 다른 목적으로 사용하지 않으며,
본 보안 정책에 따른 모든 의무를 계속 준수해야 합니다. 보관된 모든 Amazon 정보는 암호화하고 암호화된 Amazon 정보를 호스팅 또는 보관하는 대상 정보 시스템에서 암호화에 사용된 키 사본에 액세스할 수 없는 곳에 보관해야 합니다. 모든 오프라인 또는 "콜드"(즉, 바로 또는 대화식으로 사용할 수 없는) 백업은 물리적으로 안전한 시설에 저장해야 합니다.

9.4 **매체 포렌식 파기**. Amazon 정보가 포함되어 있거나 어느 때이든 포함되어 있었던 하드웨어, 소프트웨어 또는 기타 매체를 폐기하기 전에 공급업체는 NIST SP 800-88, 부록 A 에 따라 하드웨어, 소프트웨어 또는 기타 매체의 완전한 포렌식 파기를 수행해야 합니다. 이 파기 요건은 공급업체가 물리적으로 액세스하거나 통제할 수 없는 저장 매체에는 적용되지 않습니다. 이 경우 공급업체는 업계 모범 사례에 따라 더 이상 필요하지 않은 경우 Amazon 정보를 안전하게 삭제해야 합니다.

> 9.4.1 공급업체는 Amazon 으로부터 명시적으로 사전 서면 동의를 받은 경우를 제외하고 어느 때이든 Amazon 정보가 포함되어 있었던 하드웨어, 소프트웨어 또는 기타 매체를 판매, 재판매, 기증, 리퍼브 또는 달리 양도할 수 없습니다. 단, 본 조항에 따라 포렌식
> 파기를 수행한 경우에는 예외입니다.

10. **보안 검토**. Amazon 에서 요청 시 공급업체는 (a) Amazon 위험 평가를 진행하고, (b) Amazon 에서 요청한 공급업체가 본 보안 정책을 준수했음을 증명하는 증거를 제시하고, (c) Amazon 또는 Amazon 에서 지명한 제 3 자가 공급업체에서 본 보안 정책을 준수하는지 검토할 수 있도록 허용하고, 또는 (d) 4.3 항에 언급된 모든 로그 기록을 Open Cybersecurity 스키마 프레임워크(OCSF) 형식으로 Amazon 에 제공해야 합니다. 공급업체에서 Amazon 이 원격으로 검토하는 대신 직접 또는 현장 검사를 통해 증거를 검토하도록 요구하는 경우 현장 검사와 관련된 출장비 및 기타 비용은 공급업체에서 부담해야 합니다. 평가 또는 검토 결과 발견된 사항이 있는 경우 공급업체는 Amazon 이 합리적 수준으로 만족할 때까지 합의된 기간 내에 이를 시정하는 데 필요한 모든 합리적인 조치를 신속하게 취해야 하며, 이와 관련된 모든 비용은 공급업체가 단독으로 부담합니다.

11. **보안 사고.**

11.1 **보안 사고 통지**. 공급업체는 Amazon 정보 또는 대상 정보 시스템에 무단으로 액세스하거나 수집, 획득, 이용, 전송, 공개, 손상 또는 손실(이하 "보안 사고")이 발생한 사실을 알았거나 그러하다고 합리적으로 판단하는 경우 가능한 한 빨리 늦어도 24 시간 이내에 security@amazon.com 으로 보안 사고 통지를 보내 Amazon 에 이를 알려야 합니다.

11.2 **사고 대응 계획**. 공급업체는 서면 사고 대응 계획을 마련하고 요청 시 Amazon 에 사본을 제공해야 합니다. 공급업체는 서면 사고 대응 계획 및 업계 모범 사례에 따라 각 보안 사고를 적시에 해결하고, 최소 연 1 회 이상 계획을 검토 및 테스트하고 (필요한 경우) 업데이트해야 합니다.

11.3 **Amazon 에 협조.** 공급업체는 (a) Amazon 에서 보안 사고 조사 시 협조하고, (b) 보안 사고 또는 대응과 관련된 직원 및 기타 관계자와 면담할 수 있도록 지원하고, (c) 공급업체에서 진행한 보안 사고 조사 및 대응에 대한 서면 세부 사항을 보관하고, (d) Amazon 에서 요청하는 모든 관련 기록, 로그, 파일, 데이터 보고서, 포렌식 보고서, 조사 보고서 및 기타 자료를 제공해야 합니다.

11.4 **제 3 자 통지**. 법률에 달리 요구되지 않는 한 공급업체는 (a) 보안 사고를 제 3 자(규제 기관 또는 고객 포함)에게 통지하거나 (b) 보안 사고에 관한 통지 또는 공개 성명에서 Amazon 을 언급하기 전에 Amazon 으로부터 사전 서면

아래 번역은 단지 정보 제공 목적으로 제공됩니다. 이 번역본과 영문본 간에 차이, 불일치 또는 상충이 있는 경우(번역 지연 포함), 최종 업데이트된 영문본이 우선합니다.

동의를 얻어야 합니다. 법률에 달리 요구되지 않는 한 Amazon 은 보안 사고 통지를 제 3 자에게 제공할지 여부와 해당 통지의 형식, 시기 및 내용을 결정할 수 있습니다.

12. **법적 절차 통지**. 법적 절차에 대한 통지. 법으로 금지된 경우를 제외하고 법적 절차 또는 기타 관련 법률에 따라 Amazon 정보를 요청하는 경우 공급업체는 Amazon 에서 보호 명령 또는 기타 적절한 구제 수단을 모색할 수 있도록 Amazon 에 충분한 시간을 두고 이를 알려야 합니다.

13. **정의.**

13.1 "**계약**"은 본 보안 정책을 참조하는 모든 계약을 의미합니다.

13.2 "**Amazon**"은 Amazon.com, Inc. 및 그 계열사를 의미합니다.

13.3 "**Amazon 정보**"는 (a) 모든 Amazon 기밀 정보(양 당사자가 체결한 여타 계약에 명시된 정의에 따름), (b) 공급업체 또는 계열사에서 Amazon 으로부터 또는 Amazon 을 대신하여 또는 본 계약과 관련하여 달리 획득, 액세스, 수집, 수령, 저장 또는 보관하고 있는 모든 형태의 데이터, 기록, 파일, 콘텐츠 또는 정보, 및 (c) 익명 처리된 경우에도 (a) 또는 (b)에서 파생되는 정보를 의미합니다.

13.4 "**익명화**"는 Amazon 또는 사용자, 기기 식별자, 출처, 제품, 서비스, 맥락 또는 브랜드를 식별하거나 식별이 가능하게 하지 않고 달리 귀속되지 않는 방식 또는 형식으로 데이터 또는 정보(Amazon 정보 포함)를 처리하는 것을 의미합니다.

13.5 "**대상 정보 시스템**"은 공급업체에서 Amazon 정보를 처리하는 데 사용하는 모든 시스템을 의미합니다.

13.6 "**직원**"은 공급업체 또는 하청업체의 직원, 대리인, 하청업체 및 기타 시스템 및 네트워크 리소스에 대해 승인된 사용자를 의미합니다.

13.7 "**처리**"는 액세스, 사용, 수집, 수신, 저장, 변경, 전송, 배포 또는 달리 사용이 가능하게 하거나 삭제 또는 파기 등 데이터에 대해 수행하는 모든 작업을 의미합니다.

13.8 "**공급업체**"는 계약에 명시된 각 공급업체, 벤더 또는 계약업체 및 계약이 적용되는 기타 모든 제공업체를 의미합니다.