아래 번역은 정보 제공의 목적으로만 제공됩니다. 이 번역본과 영문본 사이에 차이, 불일치, 또는 상충 부분이 있는 경우, (특히 번역 지연으로 인해) 영어 버전이 우선합니다.

벤더 보안 정책

2022 년 1 월 28 일 최종 개정

1. 범위, 정의.

1.1 보안 정책. 공급업체는 본 정책(“**보안 정책**”)에서 정한 아마존의 정보 보안 요건을 모든 측면에서 준수해야 한다. 본 보안 정책은 계약에 따른 공급업체의 이행, 그리고 아마존 정보에 관한 모든 공급업체의 접근, 수집, 사용, 저장, 전송, 공개, 파기 또는 삭제 및 보안 사건에 적용된다. 본 보안 정책은 아마존과의 기타 계약 또는 공급업체에 적용되는 기타 법률에 의한 것을 포함하여 공급업체의 기타 의무, 아마존과의 기타 계약에 따른 공급업체의 이행, 아마존 정보 또는 허가된 목적을 제한하지 않는다. 본 보안 정책이 당사자들 사이의 비공개 계약이나 당사자들에 적용되는 기타 계약과 상충되는 경우, 공급업체는 신속히 아마존에 그러한 상충 내용을 통지하고 아마존 정보를 보다 잘 보호하는 요건을 준수해야 한다. 단, 덜 보호하는 요건이 더 보호하는 요건보다 우선한다고 명시적으로 언급된 경우는 그러하지 아니하다(아마존이 지정할 수 있음). 아마존은 수시로 단독 재량으로 본 보안 정책을 변경할 수 있다. 단, 그러한 변경이 상업적으로 합리적이지 않고 요청이 있을 경우 아마존은 당사자들과 만나서 적절한 추가 비용에 관해 합의해야 한다.

1.2 정의.

1.2.1 “**집계**”는 아마존의 정보를 공급업체 또는 제 3 자의 데이터 또는 정보와 결합하거나 저장하는 것을 의미한다.

1.2.2 “**계약**”은 본 보안 정책을 참조하는 일체의 계약을 말한다.

1.2.3 “**아마존**”은 Amazon.com, Inc.와 그 계열사를 의미한다.

1.2.4 “**익명화**”는 데이터 또는 정보를 아마존이나 아마존의 사용자, 기기 식별자, 출처, 제품, 서비스, 전후 사정 또는 브랜드를 식별하지도, 식별을 허용하지도, 달리 알도록 하지도 않는 방법이나 형식으로 사용, 수집, 저장, 전송 또는 변형하는 것을 의미한다.

1.2.5 “**아마존 정보**”는 (a) 모든 아마존 기밀 정보(당사자들 사이의 비공개 계약 또는 기타 계약에서 규정), (b) 공급업체 또는 그 계열사가 아마존으로부터 또는 아마존을 대리하여, 또는 본 보안 정책 또는 서비스나 계약에 따른 또는 계약과 관련된 당사자들의 이행 또는 권리의 행사와 관련하여, 공급업체 또는 그 계열사가 인수, 접근, 수집, 저장 또는 유지관리하는 일체 형태 또는 형식의 모든 기타 데이터, 기록, 파일, 내용 또는 정보, 그리고 (c) (a) 또는 (b)로부터 파생된 정보를, 개별적으로 그리고 집합적으로 의미한다(익명 처리된 경우 포함).

1.2.6 “공급업체”는 계약에서 정의된 각 공급업체, 벤더 또는 계약업체와 계약을 준수해야 할 기타 제공업체를 의미한다.

1.3 허가된 목적. 공급업체는 오직 계약에 의해 명시적으로 승인된 아마존 정보를 계약에 따른 제품 또는 서비스를 제공할 목적으로 본 보안 정책에 의해 부여된 (해당하는 경우) 라이선스에 부합하는 방법으로(“**허가된 목적**”) 접근, 수집, 사용 및 전송할 수 있다. 계약에 의하여 명시적으로 승인된 경우를 제외하고, 공급업체는 아마존 정보에 접근하거나 이를 수집, 사용, 저장 또는 전송하지 않으며 비록 익명화된 경우에도 아마존 정보를 집계하지 않는다. 아마존으로부터 사전에 명시적인 서면 동의를 받은 경우를 제외하고, 공급업체는 (a) 아마존 정보를 이전, 대여, 교환, 거래, 판매, 대출, 리스 또는 달리 배포하거나 제 3 자가 이용할 수 있도록 하지 않으며, (b) 비록 익명화된 경우에도 아마존 정보를 다른 정보와 함께 집계하지 않는다.

2. 아마존 보안 정책.

2.1 기본 보안 요건. 공급업체는 현행 최고의 업계 표준과 아마존 정보의 분류 및 민감성에 기초하여 아마존이 명시한 기타 요건에 부합하게 물리적, 행정적, 기술적 보호 장치 및 기타 보안 조치를 유지하여, (a) 공급업체가 접근, 수집, 사용, 저장 또는 전송하는 아마존 정보의 보안 및 기밀성을 유지하고, (b) 정보를 보안 및 무결성, 사고에 의한 분실, 변형, 공개 및 기타 모든 불법적인 형태의 처리에 대해 알려졌거나 합리적으로 예상할 수 있는 위협 또는 위험 요소로부터 보호한다. 어떤 경우에도, 공급업체는 아마존 정보를 처리하기 위하여 또는 접근하기 위하여 사용하는 시스템("아마존 정보 시스템")에 대한 다음 요건을 준수해야 한다.

2.1.1 네트워크 보안. 공급업체는 특히 외부 인터넷으로부터의 무단 네트워크 접속을 제한함으로써 아마존 정보 시스템을 보호한다. 공급업체는 방화벽과 같은 효과적인 네트워크 보안 솔루션을 설치하고 유지하여 항상 아마존 정보를 보호한다.

2.1.2 업데이트. 국립표준기술연구소("NIST") 특별판("SP") 800-40 개정본 3 에 약술된 바와 같이, 공급업체는 아마존 정보 시스템을 아마존 정보의 보안을 확보하는 데 필요한 최근 업그레이드, 업데이트, 버그 수정, 신규 버전 및 기타 수정을 통하여 최신 상태로 유지한다.

2.1.3 안티-멀웨어. 공급업체는 항상 안티-멀웨어 소프트웨어 또는 그에 상응하는 보안 통제를 사용하여 멀웨어 침해 및 확산 위험을 완화한다. 사용하는 경우, 공급업체는 안티-멀웨어 소프트웨어를 최신 상태로 유지한다.

2.1.4 암호화. 공급업체는 업계 모범관행에 따라 저장 중인 데이터와 공공 네트워크를 통해 전송되는 데이터를 암호화한다.

2.1.5 테스트. 공급업체는 정기적으로 보안 시스템 및 프로세스를 테스트하여 그러한 보안 시스템 및 프로세스가 본 보안 정책 또는 공급업체와 아마존이 마지막으로 합의한 보안 정책의 요건을 충족하도록 한다. 섹션 1.1 에 따라 보안 정책에 변경이 있는 경우, 그러한 변경은 공급업체와 아마존이 합의(이메일도 충분)할 때까지 본 섹션의 목적상 효력이 없다.

2.1.6 접근 통제. 공급업체는 다음 요건의 준수를 포함하여 아마존 정보의 보안을 유지한다.

2.1.6.1 공급업체는 아마존 정보 또는 아마존 정보 시스템에 대한 컴퓨터 접속 권한을 가진 각각의 사람에게 고유한 ID 를 배정한다.

2.1.6.2 공급업체는 아마존 정보에 대한 접속 권한을 허가된 목적을 위해 "알 필요"가 있는 사람들로만 제한한다.

2.1.6.3 공급업체는 정기적으로 아마존 정보에 대한 접속 권한을 가진 사람 및 서비스의 목록을 검토하여 더 이상 아마존 정보 시스템에 접속이 불필요한 계정을 제거한다. 이러한 검토는 최소 90 일에 한 번 실시한다.

2.1.6.4 공급업체는 아마존 정보 시스템에서의 시스템 비밀번호 및 기타 보안 파라미터에 대하여 제조사가 공급한 기본 비밀번호를 사용하지 않는다. 공급업체는 모든 아마존 정보 시스템에서 NIST SP 800-63B 에 기술된 모범관행에 따라 시스템이 강제하는 "강력한 비밀번호" 사용을 의무화하고 이를 확인한다. 공급업체는 모든 비밀번호 및 접속 권한 자격 증명이 기밀로 유지되고 직원 간에 공유되지 않도록 한다.

2.1.6.5 공급업체는 계정에 연속해서 십(10) 회 이상 틀린 비밀번호를 시도하는 경우, 아마존 정보 또는 아마존 정보 시스템에 대한 접속 권한을 가진 계정을 비활성화하여 "계정 잠금" 상태를 유지하고 이를 강제해야 한다.

2.1.6.6 아마존이 서면을 통해 명시적으로 승인한 경우를 제외하고, 공급업체는 아마존 정보를 항상(저장, 처리 또는 전송 포함) 공급업체 및 제 3 자의 정보로부터 물리적으로, 그리고 논리적으로 분리해야 한다.

2.1.6.7 아마존이 서면으로 물리적 통제를 추가로 요청한 경우, 공급업체는 그러한 안전한 물리적 접근 통제 조치를 실시하고 사용해야 한다.

2.1.6.8 아마존이 합리적으로 요청하는 즉시, 공급업체는 아마존에 (a) 허가된 목적으로 공급업체에 제공된 아마존의 계정 또는 자격 증명(예: 소셜 미디어 계정 자격증명)의 모든 사용에 관한 일지 데이터, (b) 아마존 정보에 대한 접근 권한을 가진 아마존 직원 또는 공급업체의 직원 사칭 또는 사칭 시도에 관한 상세한 일지 데이터를 제공한다.

2.1.6.9 공급업체는 정기적으로 악의적인 행위 또는 무단 접속 징후를 찾기 위해 접속 일지를 검토한다.

2.1.7 공급업체의 정책. 공급업체는 정책 위반을 탐지하고 기록하는 방법을 포함하여 직원, 계약직원, 에이전트, 그리고 본 보안 정책에서 정한 기준을 충족하는 공급업체에 적용되는 정보 및 네트워크 보안 정책을 유지하고 집행한다. 공급업체의 정보 및 네트워크 보안 정책의 위반이 보안 사건(아래에 정의)에 해당된다고 공급업체 또는 아마존이 합리적으로 의심할 만하여 아마존이 요청하는 경우, 공급업체는 아마존에 이에 관한 정보를 제공한다.

2.1.8 하도급 계약. 공급업체는 아마존의 사전 서면 동의 없이 본 보안 정책에 따른 의무를 하도급업체 또는 대리인(“**하도급업체**”라 총칭함)에 하청을 주거나 위임하지 않는다. 하도급 계약 또는 위임의 존재 또는 그러한 조건에도 불구하고, 공급업체는 계속해서 본 보안 정책에 따른 의무를 완전히 이행할 책임을 진다. 본 보안 정책의 조건은 공급업체의 하도급업체 및 직원에 구속력이 있다. 공급업체는 (a) 하도급업체 및 직원이 본 보안 정책을 준수하도록 하고, (b) 공급업체의 하도급업체 및 직원의 모든 작위, 부작위, 과실 및 불법행위에 대하여 책임을 진다.

2.1.9 원격 접속. 공급업체는 아마존 정보 시스템에 접속하려면 다중 요소 인증(예: 사용자를 식별하기 위한 최소 두 개의 별개 요소)을 거치도록 한다.

2.1.10 ”대량” 접속. 본 섹션의 목적상 “대량” 접속이란 데이터베이스 질의, 보고서 생성 또는 기타 데이터 대량 이전 수단에 의해 데이터에 접속하는 것을 말한다. 서면을 통해 아마존이 명시적으로 승인한 경우를 제외하고, 공급업체는 아마존 정보에 “대량”으로 접속하지 않으며 접속을 허용하지도 않는다. 이는 아마존 정보가 공급업체나 아마존이 통제하는 데이터베이스에 있든, 파일 기반 아카이브에의 저장을 포함한 기타 방법에 의한 저장이든 상관이 없다. 구체적으로 말하면, 본 섹션은 허가된 목적에 필요하여 개별 기록에 접속하는 경우를 제외하고 아마존 정보에 대한 접속을 금지한다. 공급업체는 아마존 정보에 대한 “대량” 접속 시도 또는 그 성공에 대하여 상세한 일지 데이터를 보존하고 섹션 2.5(보안 검토)에 의한 공급업체의 의무 일부로서 이러한 일지에 대한 보고서를 제공한다. 아마존이 공급업체에 아마존 정보에 대한 “대량” 접속을 서면으로 승인하는 경우, 공급업체는 (a) 그러한 접속을 “알 필요”가 있는 특정 직원으로만 제한하고, (b) 도구를 사용하여 접속을 제한하고, 명확히 승인하고, 모든 접속을 기록한다.

2.1.11 공급업체 직원. 아마존이 명시한 형식의 개별적인 비공개 계약을 체결하여 아마존에 인도하는 경우에 한해 아마존은 공급업체 직원이 아마존 정보에 접근하는 것을 허용한다. 아마존이 요구하는 경우 공급업체 직원은 개별적인 비공개 계약을 체결할 수 있다 공급업체는 아마존 정보에 대한 접속 권한을 받을 공급업체 직원으로부터 서명된 개별 비공개 계약을 받아서 아마존에 인도한다(공급업체 직원에 접속 권한을 부여하거나 정보를 제공하기 전에). 또한 공급업체는 아마존 정보 시스템에서 아마존 정보에 접근하거나 수령한 모든 공급업체 직원의 명단을 유지하고, 요청하는 경우 그 명단을 아마존에 신속히 제공한다. (a) 아마존 정보에 더 이상 접근할 필요가 없거나, (b) 더 이상 공급업체 직원 자격이 없는(예: 공급업체를 퇴사한 개인) 공급업체 직원의 경우, 공급업체는 즉시(최대 24 시간 이내에) 아마존 정보 및 아마존 정보 시스템에 대한 접근 권한을 종료시킨다. 그러한 직원에게 아마존 정보 시스템에서 아마존 정보에 접근할 수 있는 권한이 주어지는 경우에도, 공급업체는 24 시간 이내에 아마존에 통보한다.

2.2 아마존 엑스트라넷 및 공급업체 포털 접속. 아마존은 허가된 목적을 위해 아마존의 또는 제 3 자의 웹사이트 또는 시스템의 웹 포털 또는 기타 비공개 웹사이트 또는 엑스트라넷 서비스(각각 “**엑스트라넷**”)를 통한 아마존 정보에 대한 접근 권한을 공급업체에 부여할 수 있다. 아마존이 엑스트라넷을 사용하여 아마존 정보에 대한 접속 권한을 허가하는 경우 공급업체는 다음 요건을 준수해야 한다.

2.2.1 허가된 목적. 공급업체와 공급업체 직원은 허가된 목적을 위해서만 엑스트라넷에 접속하여 아마존 정보에 접속하고 이를 수집, 사용, 열람, 검색, 다운로드 또는 저장한다.

2.2.2 계정. 공급업체는 공급업체 직원으로 하여금 아마존이 각 개인에게 지정한 엑스트라넷 계정만을 사용하도록 하고, 공급업체 직원에게 접속 자격 증명을 기밀로 유지하도록 요구해야 한다.

2.2.3 시스템. 공급업체는 자신이 관리하는 운영 시스템을 구동하는 컴퓨팅 또는 프로세싱 시스템 또는 애플리케이션만을 통하여 엑스트라넷에 접속한다. 여기에는 (a) 섹션 2.1.1(네트워크 보안)에 따른 시스템 네트워크 방화벽, (b) 섹션 2.1.2(업데이트)를 준수하는 중앙집중식 패치 관리, (c) 섹션 2.1.3(안티 멀웨어)에 따라 운영 시스템에 적절한 안티 멀웨어, (d) 휴대용 기기용 완전한 디스크 암호화가 포함된다.

2.2.4 제약사항. 아마존이 서면으로 사전에 승인한 경우를 제외하고, 공급업체는 엑스트라넷으로부터 아마존 정보를 기계, 기기 또는 서버를 포함하여 어떠한 매체에도 다운로드, 복사, 영구히 저장하지 않는다.

2.2.5 계정 해지. 공급업체는 엑스트라넷에 대한 접속 권한을 가진 공급업체 직원이 (a) 아마존 정보에 대한 접속이 더 이상 필요없게 되거나, (b) 직원 자격이 없어진 뒤(예: 직원의 공급업체 퇴사) 24 시간 이내에 그러한 직원의 계정을 해지하고 이를 아마존에 통보한다.

2.2.6 제 3 자 시스템.

2.2.6.1 공급업체는 아마존에 사전 통지를 하고 아마존의 사전 서면 승인을 받은 후 제 3 자 시스템을 사용하여 아마존 정보를 저장하거나 아마존 정보에 접속할 수 있다. 단, (a) 데이터가 본 보안 정책에 따라 암호화되고, (b) 제 3 자 시스템이 데이터의 복호 키 또는 암호화되지 않은 '평이한 문장" 버전에 접속하는 경우에는 그러하지 아니하다. 아마존은 승인하기 전에 제 3 자 시스템에 대해 섹션 2.5(보안 검토)에 따른 아마존 보안 검토를 요구할 권리를 갖는다.

2.2.6.2 공급업체가 암호화되지 않은 아마존 정보를 저장하거나 암호화되지 않은 아마존 정보에 접속할 수 있는 제 3 자 시스템을 사용하는 경우, 공급업체는 제 3 자 시스템 및 보안 통제에 대해 보안 검토를 실시하고 아마존이 요구하는 형식(예: SAS 70 또는 그 후속 보고서, 또는 아마존이 승인한 기타 인정된 업계 표준 보고서)으로 제 3 자 시스템의 보안 통제에 관한 정기 보고서를 아마존에 제공한다.

2.3 데이터 보관 및 파기.

2.3.1 보관. 공급업체는 아마존 정보를 허가된 목적을 위해서만, 그리고 허가된 목적에 필요한 기간 동안만 보관한다.

2.3.2 반환 또는 삭제. 아마존의 요청을 받으면 공급업체는 반환 및/또는 삭제를 요구하는 아마존의 통지에 따라 신속히(그러나 72 시간 이내에) 모든 아마존 정보를 아마존에 반환하고 영구히, 그리고 안전하게 이를 삭제한다. 공급업체는 또한 허가된 목적 달성과 본 보안 정책의 해지 또는 만료 중 일찍 도래하는 날로부터 30 일 이내에 아마존 정보의 모든 라이브(온라인 또는 네트워크를 통해 접속 가능한) 사례를 영구히, 그리고 안전하게 삭제한다. 아마존이 요구하는 경우, 공급업체는 모든 아마존 정보가 파기되었음을 서면으로 증명한다. 명확히 하자면, 본 섹션은 섹션 2.3.3 에 따른 아카이브 사본에는 적용되지 않는다.

2.3.3 아카이브 사본. 법률에 의해 공급업체가 세금 또는 이와 비슷한 규제 목적상 아마존 정보의 아카이브 사본을 보관해야 하는 경우, 아마존의 아카이브 정보는 다음 중 하나의 방법으로 보관되어야 한다.

2.3.3.1 물리적 보안이 확보된 시설에 "콜드" 또는 오프라인(예: 즉시 또는 쌍방향 사용에 필요하지 않은) 백업 보관으로 보관, 또는

2.3.3.2 암호화된 파일을 호스팅하거나 보관하는 시스템이 암호화에 사용된 키의 사본에 접근하지 못하는 경우 암호화하여 보관.

2.3.4 복구. 공급업체가 재난 복구 목적으로 "복구"(예: 백업으로 전환)를 실시하는 경우, 공급업체는 계약 또는 본 보안 정책이나 아마존과의 기타 계약에 따라 삭제하여야 할 모든 아마존 정보가 본 섹션 2.3 에 따라 복구된 후 24 시간 이내에 다시 삭제되거나 겹쳐 쓰기가 이루어지도록 하는 프로세스를 준비하고 유지해야 한다. 공급업체가 어떤 목적으로 복구를 실시하는 경우, 아마존의 사전 서면 승인 없이는 어떤 아마존 정보도 제 3 자 시스템이나 네트워크로 복구할 수 없다. 아마존은 아마존 정보를 제 3 자 시스템 또는

네트워크로의 복구를 허가하기 전에 제 3 자 시스템 또는 네트워크에 대한 아마존의 보안 검토(섹션 2.5(보안 검토)에 따른)를 요구할 권리가 있다.

2.3.5 데이터 위생처리 기준. 공급업체가 삭제하는 모든 아마존 정보는 2014 년 12 월 18 일에 발표된 NIST SP 800-88 수정본 1, 미디어 위생처리 가이드라인(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf), 관련 유형의 기기 제거 목적을 위한 부록 A 에 포함된 최소 위생처리 권고사항에 따라 삭제된다. NIST SP 800-88, 부록 A 에 관련 지침이 없는 경우, 아마존 정보가 담긴 기기는 (a) 10,000+ 가우스 이상의 전자기가 흐르는 장소에서 자기 매체를 소자하는 방식으로, 또는 (b) 2x2mm 보다 작은 입자로 파쇄하거나 기계적으로 해체하는 방식으로, 또는 (c) 아마존 정보의 분류 및 민감도를 기준으로 아마존이 요구할 수 있는 기타 기준에 따라 파기되어야 한다.

2.4 포렌식 파기. 아마존 정보를 포함하고 있거나 있었던 하드웨어, 소프트웨어 또는 기타 일체의 매체를 (어떠한 방법으로든) 처분하기 전에, 공급업체는 아마존 정보를 어떠한 형식으로도 검색할 수 없도록 하드웨어, 소프트웨어 또는 기타 매체를 완전하게 포렌식 방법으로 파기한다. 공급업체는 관련 유형의 기기 파기에 대한 NIST SP 800-88, 부록 A 에 포함된 최소 위생처리 권고사항에 따라 포렌식 파기를 실시한다.

2.4.1 공급업체는 섹션 2.4 에서 요구하는 대로 공급업체가 포렌식 방법으로 파기하지 않은 아마존 정보가 담긴 하드웨어, 소프트웨어 또는 기타 매체를 판매, 재판매, 기증, 재단장 또는 이전하지 않는다(하드웨어, 소프트웨어, 기타 매체의 판매 또는 이전, 공급업체의 사업의 청산과 관련한 처분, 또는 기타 처분 포함).

2.5 보안 검토.

2.5.1 아마존은 아마존 위험 평가에 참가할 것을 공급업체에 정기적으로 요구할 권리가 있다.

2.5.2 증명. 아마존이 서면으로 요청하는 경우, 공급업체는 서면으로 아마존에 위험 평가의 일환으로 제공된 정보가 공급업체와 아마존이 마지막으로 합의한 본 보안 정책을 준수하고 있다는 점을 증명한다. 섹션 1.1 에 따라 보안 정책에 변경이 있는 경우, 그러한 변경은 공급업체와 아마존이 합의(이메일도 충분)할 때까지 본 섹션의 목적상 효력이 없다.

2.5.3 기타 검토. 아마존은 아마존 정보 시스템의 보안을 정기적으로 검토할 권리를 갖지만 (a) 달력 기준으로 그 해에 상당한 하자가 이전에 발견되었거나, (b) 아마존이 정부기관 또는 기타 규제기관에 의해 그러한 검토를 실시할 의무가 있는 경우가 아니면 연간 한 번을 초과하면 안 된다. 공급업체는 합리적인 기간 내에, 그러나 아마존이 요청한 날로부터 역일 기준 20 일 이내에 협력하고 모든 요청 정보를 아마존에 제공한다.

2.5.4 시정. 보안 검토를 통해 결함이 발견된 경우, 공급업체는 공급업체가 비용 및 경비를 전액 부담하여 합의된 기간 내에 이러한 결함을 시정하는 데 필요한 합리적인 모든 조치를 취한다.

2.6 보안 사건.

2.6.1 공급업체는 실제 또는 의심스러운 아마존 정보의 무단 접속, 수집, 획득, 사용 전송, 공개, 변형 또는 분실이나 아마존 정보 시스템의 침해(**"보안 사건"**)를 알게 된 후 가능한 한 신속히, 그러나 24 시간 이내에 아마존에 알린다. 공급업체는 제때에 각 보안 사건을 시정하고 아마존에 각 보안 사건에 관한 공급업체의 내부 조사에 대한 상세한 내역을 서면으로 제공한다, 해당 법률에 의하여 허용되는 경우, 아마존이 특별히 서면으로 공급업체에 요청하지 않는 한 공급업체는 아마존을 대신하여 규제당국이나 고객에 통지하지 않는다는 데 동의한다. 아마존은 당사자에게 제공하기 전에 통지의 형식과 내용을 검토하고 승인할 권리를 갖는다. 공급업체는 아마존과 협조하고 협력하여 확인된 모든 보안 사건을 시정하기 위한 계획을 세우고 이를 실행한다.

2.6.2 해당 법률이 허용하는 범위 내에서, 공급업체가 정부기관으로부터 아마존 정보가 포함된 데이터를 구하는 요구 또는 명령(예: 소환장, 법원 명령 또는 수색 영장)을 받는 경우, 공급업체는 아마존이 보호 명령 또는 기타 적절한 구제책을 마련할 수 있도록 아마존에 충분한 통지를 제공한다.

2.7 일반 사항. 아마존은 본 보안 정책에 따라 모든 해당 결정을 할 수 있는 단독 재량권을 갖는다. "포함하는" 또는 "예" 다음에 나오는 목록은 예시적인 것으로 모든 것을 포괄하는 것은 아니다. 본 보안 정책에 따른 보안 요건의 기준에

대한 모든 언급은 아마존이 달리 명시하지 않는 한 특정 기준과 업데이트될 수 있는 각각의 후속 버전 또는 그에 상응하는 버전을 지칭한다.