본 계약의 영문 버전을 보려면 여기를 클릭하십시오. 이 영문 버전이 법적 구속력을 가지며, 국문 버전은 참조 목적입니다.

Dell APEX 파트너 데이터 처리 부록

본 계약에 대한 Dell APEX 파트너 데이터 처리 부록("**파트너 DPA**")은 본 계약의 양 당사자가 Dell의 서비스 제공("**서비스**")을 포함하여 본 계약에 따른 의무를 이행하는 과정에서 개인 정보를 교환할 수 있는 경우에 적용됩니다. 본 파트너 DPA와 본 계약이 상충하는 경우에는 계약 주제에 관련하여 본 파트너 DPA가 우선합니다.

1. 정의.

본 부록에서 정의되지 않은 용어는 본 계약에 규정된 의미를 가집니다. 본 파트너 DPA에서 다음 용어는 다음과 같은 의미를 가집니다.

1.1 "본 계약"은 Dell APEX 리셀러 계약, Dell APEX 총판 계약 또는 이와 실질적으로 유사하며 Dell의 서비스 제공에 대한 근거가 되는 계약을 의미합니다.

1.2 "정보통제권자"는 단독으로 또는 타인과 공동으로 개인 정보 처리의 목적 및 수단을 결정하는 주체를 의미합니다.

1.3 "GDPR"은 일반 데이터 보호 규정(EU) 2016/679를 의미합니다.

1.4 해당되는 경우 "모델 조항"은 다음을 의미합니다.

(i) 개인 정보 전송에 대한 표준 계약 조항(결정 2021/914/EU). 이는 유럽 경제 지역("**EEA**")에서 제 3 국으로의 전송과 관련되어 있으며 수시로 수정되거나 대체될 수 있습니다.

(ii) 유럽 위원회의 국제 데이터 전송에 관한 표준 계약 조항에 대한 국제 데이터 전송 부록 또는 국제 데이터 전송 협정. 이들은 영국("**UK**")에서 UK GDPR 에 따른 적절성 결정이 적용되지 않는 국가로의 전송과 관련하여 2018 년 정보보호법 제 119A 조에 따라 각각 발행되었습니다.

(iii) 개인 정보 전송에 대한 표준 계약 조항(결정 2021/914/EU). 이는 수시로 수정 또는 대체될 수 있으며, 스위스에서 제 3 국으로의 전송과 관련하여 2021 년 8 월 27 일 스위스 연방 데이터 보호•정보 위원회가 공표한 개정안에 근거하여 스위스 연방 정보보호법에 따른 목적을 위해 특별히 수정되었습니다.

1.5 "개인 정보"는 식별되거나 식별 가능한 자연인 관련 정보 또는 개인 정보 보호법에 따라 "개인 데이터" 또는 "개인 정보"로 달리 정의된 정보를 의미합니다. 이러한 개인 정보는 계약을 이행하는 양 당사자에 의해 처리됩니다.

1.6 "개인 정보 침해"는 본 파트너 DPA에 따라 처리된 개인 정보의 우발적 또는 불법적인 파괴, 손실, 변경, 무단 공개 또는 해당 정보로의 액세스를 유발하는 보안 위반을 의미합니다.

1.7 "개인 정보 보호법"은 해당되는 경우, GDPR, 영국 GDPR, 캘리포니아 소비자 개인 정보 보호법("CCPA"), 기타 유사한 법률을 포함하여 본 계약의 당사자와 제공된 서비스에 적용되는 모든 데이터 보호 및 개인 정보 보호법을 의미합니다.

1.8 "처리"는 자동화 수단에 의한 것인지에 관계없이 수집, 기록, 정리, 구조화, 저장, 수정 또는 변경, 검색, 조회, 사용, 전송에 의한 공개, 배포나 기타 방법에 의한 제공, 정렬이나 조합, 제한, 삭제 또는 폐기 등 개인 정보 또는 일련의 개인 정보에서 수행되는 모든 작업이나 일련의 작업을 의미합니다.

1.9 "정보처리자"는 정보통제권자를 대리하여 개인 정보를 처리하는 주체를 의미합니다.

1.10 "판매"는 기업에서 금전적 또는 비금전적 대가를 위해 다른 기업이나 제 3 자에게 소비자의 개인 정보를 구두, 서면, 전자 또는 기타의 방식으로 판매, 대여, 발표, 공개, 배포, 제공, 전송 또는 전달하는 것을 의미합니다. 공개

정보통제권자가 계약에서 정하는 당사자들의 의무를 이행하기 위해 수신 정보통제권자에게 개인 정보를 공유하거나 전송하는 것은 판매에 포함되지 않습니다.

1.11 "하위 정보처리자"는 정보처리자 역할을 하는 일방 당사자(계열사 및/또는 수급 사업자를 포함하되 이에 국한되지 않음)가 본 파트너 DPA에 따른 개인 정보 처리를 위해 고용한 제3자를 의미합니다.

1.12 "영국 GDPR"은 영국의 유럽 연합 탈퇴로 영국 국내법에 따라 유지되는 GDPR(2018 영국 정보보호법과 함께 해석하여 적용)을 의미하며, 수시로 개정될 수 있습니다.

2. 규정 준수

양 당사자는 본 계약에 따라 고려된 관계에 적용되는 관련 개인 정보 보호법에 따른 의무를 준수하며 관련 개인 정보 보호법에 따라서만 개인 정보를 처리할 것에 동의합니다. 각 당사자는 상대방 당사자에게 개인 정보를 공개, 전송 또는 기타 방식으로 제공하기 전에 개인 정보 처리의 적법성과 관련하여 개인 정보 보호법을 준수할 의무가 있으며, 상대방 당사자에게 개인 정보를 공개하는 데 필요한 모든 권리와 권한을 취득했어야 합니다(적절한 알림 제공, 필요한 경우 본 계약과 관련한 개인 정보 공개에 대해 개인 정보 보호법에 따른 정보주체의 동의 획득 등이 포함되며 이에 국한되지 않음).

3. 정보통제권자 간 개인 정보 공개

정보통제권자 역할을 하는 일방 당사자("공개 정보통제권자")가 정보통제권자로서 정보를 처리하는 상대방 당사자("수신 정보통제권자")에게 개인 정보를 공개할 경우 다음과 같은 의무가 적용됩니다.

3.1 양 당사자가 서면으로 달리 합의하지 않는 한, 수신 정보통제권자는 관련 개인 정보 보호법에 따라 본 계약에 따른 의무를 이행하기 위한 목적으로만 개인 정보를 처리합니다. 수신 정보통제권자는 개인 정보 보호법에 명시적으로 허용되지 않은 활동이나 목적으로 개인 정보를 처리해서는 안 됩니다.

3.2 개인 정보는 본 계약에 따른 의무를 이행하기 위한 목적으로만 수신 정보통제권자에게 제공됩니다. 공개 정보통제권자는 계약에 따라 서비스를 이행하기 위해 본 계약에 따라 합의된 대가를 지불하는 경우를 제외하고 개인 정보를 이용하거나 달리 처리하기 위해 금전적 또는 기타 비금전적 대가를 제공하지 않습니다.

3.3 공개 정보통제권자는 수신 정보통제권자의 마케팅 통신 전송 목적을 위해 개인 정보를 공개할 경우, 수신 정보통제권자의 해당 공개 및 사용에 관해 관련 정보주체의 사전 동의를 얻을 것에 동의합니다.

3.4 각 당사자는 개인 정보와 관련하여 정보주체의 개인 정보 보호법에 따른 권리 행사 요청(접근, 제한, 수정, 삭제 및 이동에 대한 동의를 철회할 권리 포함)에 응답할 의무를 즉시 이행해야 합니다. 수신 정보통제권자는 수신 정보통제권자의 관행, 절차 및/또는 이의 제기 절차 관련 정보 및 개인 정보에 대한 접근 또는 수정 요청을 비롯하여 개인 정보와 관련한 공개 정보통제권자 또는 정보주체의 모든 합당한 문의를 즉시 처리합니다.

3.5 일방 당사자는 제 3 자(데이터 보호 감독 기관 포함)의 요청 또는 통지를 받거나 본 계약에 따라 처리된 개인 정보와 관련한 법원의 명령을 받은 경우, 모든 관련 정보를 제공하여 상대방 당사자에게 즉시 통지해야 합니다. 양 당사자는 그런 요청 또는 알림에 대응하기 위해 합리적으로 상호 협력해야 합니다. 법률에서 요구하는 경우를 제외하고 양 당사자는 상대방 당사자의 서면 지시 없이 상대방 당사자를 대신하여 요청 또는 알림에 응답해서는 안 됩니다.

3.6 계약과 관련하여 개인 정보 침해가 발생한 경우 개인 정보 침해를 당한 당사자는 이를 인지한 후 지체 없이 상대방 당사자에게 알려야 합니다. 각 당사자는 상호 협력하고 상대방 당사자가 개인 정보 침해를 처리, 완화 및/또는 해결하도록 지원해야 합니다. 양 당사자는 상호 협의에 따라 관련 감독 기관 및/또는 정보주체에 통지할 개인 정보 보호법에 따른 의무를 준수해야 합니다.

3.7 수신 정보통제권자는 계약의 목적상 개인 정보를 더 이상 유지할 필요가 없거나 관련 법률에서 달리 요구하는 경우 계약이 종료된 후 개인 정보를 삭제 및/또는 파기해야 합니다.

3.8 수신 정보통제권자는 (i) 개인 정보 판매, (ii) 계약에 따른 의무를 이행하는 특정 목적 이외의 다른 목적으로 개인 정보를 유지, 사용 또는 공개(계약을 이행하는 이외의 상업적 목적으로 개인 정보를 유지, 사용 또는 공개하는 경우를

포함하되 이에 국한되지 않음), (iii) 공개 정보통제권자와 수신 정보통제권자 간의 직접적인 사업 관계 이외의 목적으로 개인 정보를 유지, 사용 또는 공개하는 행위가 금지됩니다.

3.9 수신 정보통제권자는 개인 정보와 관련하여 본 파트너 DPA, 특히 제 3.8 항에 요약된 관련 목적과 개인 정보의 사용 및 모든 다른 처리 활동에 관한 금지 및 제한 사항을 이해하고 이를 준수할 것을 진술하며 이를 보증합니다.

4. 정보통제권자가 정보처리자에게 개인 정보 공개

정보통제권자 역할을 하는 일방 당사자가 정보처리자 또는 하위 정보처리자 역할을 할 상대방 당사자에게 개인 정보를 공개할 경우 정보처리자 또는 하위 정보처리자 역할을 하는 당사자는 다음와 같이 해야 합니다.

4.1 관련 법률에서 요구하지 않는 한 정보통제권자의 지시에 따라서만 개인 정보를 처리합니다. 파트너 DPA 에 포함되지 않은 추가 또는 대체 처리 지시는 양 당사자가 해당 지시의 준수에 관련된 비용(발생하는 경우)을 포함하여 서면으로 합의해야 합니다. 양 당사자는 정보통제권자의 지시가 해당 법률을 준수하는지 판단할 책임이 없습니다. 그러나 정보통제권자의 지시가 해당 개인 정보 보호법을 침해한다고 판단되는 경우에 일방 당사자는 이를 합리적으로 가능한 한 신속하게 상대방 당사자에게 통지해야 하며, 상기의 법률 침해 지시를 준수해야 할 의무가 없습니다. 처리의 주제, 기간, 성격 및 목적, 개인 정보 및 정보주체의 유형 등에 대한 세부 사항이 계약 및 별지 2 에 규정되어 있습니다.

4.2 본 계약에 따른 의무를 이행하는 데 필요한 경우에만 정보통제권자가 제공한 개인 정보를 처리합니다.

4.3 다음 목적에 한해 필요한 경우를 제외하고 계열사 또는 하위 정보처리자 이외의 제 3 자에게 개인 정보를 공개해서는 안 됩니다.

(a) 정보통제권자의 지시 준수

(b) 파트너 DPA 준수

(c) 법률 또는 정부 기관의 구속력 있는 명령 준수 법률 또는 정부 기관의 구속력 있는 명령을 위반하지 않는 한 정보처리자는 본 규정에 참조되는 법적 요구 사항 또는 명령에 대해 정보통제권자에게 통지합니다.

4.4 개인 정보 침해를 알게 된 경우 (i) 정보통제권자에게 지체 없이(72시간 이내에) 통지하고, (ii) 해당 시점에 관련 정보가 정보처리자에게 알려져 있거나 제공된 경우 개인 정보 침해에 대한 세부 사항을 서면으로 제공하고, (iii) 상대방 당사자가 개인 정보 침해의 역효과를 완화하도록 돕기 위해 합당한 노력을 하며(가능한 경우), (iv) 해당 개인 정보 침해와 관련하여 개인 정보 보호법에 요구된 모든 조치를 이행합니다.

4.5 합당한 사전 서면 요청이 있는 경우 관련 법률에 따라 정보처리자의 본 파트너 DPA 규정 준수를 입증하는 데 합리적으로 필요할 수 있는 정보를 정보통제권자에게 제공합니다.

4.6 합당한 사전 통지를 받은 경우 정보처리자 역할을 하는 일방 당사자의 개인 정보 처리와 관련하여 개인 정보 보호법에 요구된 범위 내에서 데이터 보호 영향 평가 및/또는 사전 협의를 실시하기 위해 합당하게 요청된 지원을 정보통제권자에게 제공합니다.

4.7 관련 개인 정보 보호법에 따른 권리를 행사하려는 개인의 요청을 포함한 계약에 따른 개인 정보 처리와 관련된 개인 또는 관련 데이터 보호 기관의 요청에 대해 정보통제권자에게 즉시 통지하고 정보통제권자와 협력하여 해결합니다. 정보처리자는 법적으로 요구되는 경우를 제외하고 정보통제권자의 사전 승인 없이 해당 통신에 직접 회신해서는 안 됩니다.

4.8 계약이 만료 또는 해지되거나 정보통제권자가 서면 등으로 달리 요청한 경우 합당하게 실행 가능한 가장 이른 시간에 모든 개인 정보를 삭제하거나 정보통제권자에게 반환합니다. 단, 정보처리자가 관련 법률에 따라 복사본을 유지해야 하는 경우 정보처리자는 관련 법률에서 요구하는 경우를 제외하는 범위에서 추가적인 처리를 제한하여 개인 정보를 보호합니다.

4.9 일방 당사자는 CCPA의 범위 내에 속하는 개인 정보를 처리하는 경우 상대방 당사자를 대리하여 개인 정보를 처리해야 하며, 개인 정보를 본 파트너 DPA에 규정되고 CCPA나 그 후속 법률에 따라 허용된 목적 이외의 목적으로

보유, 사용, 공유 또는 공개하지 않아야 합니다. 어떠한 경우에도 양 당사자는 개인 정보를 제3자(아래 제5조에 따른 하위 정보처리자 제외)와 공유하거나 개인 정보를 판매해서는 안 됩니다. 각 당사자는 상대방 당사자가 CCPA에 따라 개인 데이터 또는 개인 정보를 판매한 것으로 간주되는 어떠한 행위도 하지 않는 것을 포함하여 개인 정보 처리 시 적용되는 모든 제한 사항을 이해하고 준수할 것임을 확인합니다. 이 항의 목적을 위해 본 계약의 정보처리자는 CCPA 제1798.140항(v)에 정의된 서비스 제공자로 간주됩니다.

4.10 상대방 당사자의 합당한 사전 서면 요청을 받은 경우(계약 약관에 따라 요청된 경우) 본 파트너 DPA에 따른 정보처리자의 의무 이행을 입증하는 데 필요한 정보를 제공하고 상대방 당사자 또는 상대방 당사자가 위임한 다른 감사자에 의한 감사(사찰 포함)를 허용하고 협조해야 합니다.

5. 하위 정보처리자.

5.1 하위 정보처리자의 사용.

각 당사자는 상대방 당사자에게 하위 정보처리자 사용에 대한 일반적인 동의를 받을 수 있습니다. 양 당사자는 본 계약에 따라 서비스와 관련하여 개인 정보를 처리하기 위해 하위 정보처리자를 위임하고 사용할 수 있습니다. 어느 경우든 하위 정보처리자가 제공할 서비스와 관련하여 각 하위 정보처리자와 서면으로 계약을 체결하고, 해당 계약에 따라 하위 정보처리자는 (i) 적절한 기술적 조직적 조치를 이행하는 데 충분한 보증을 제공하고, (ii) 본 파트너 DPA에 따라 Dell에 부과되는 권리 및/또는 의무와 물리적으로 유사한 조건을 준수해야 합니다. 하위 정보처리자는 제3자 또는 각 당사자의 계열사를 포함할 수 있습니다. 하위 정보처리자가 위에 규정된 데이터 보호 의무를 이행하지 못한 경우, 해당 하위 정보처리자를 고용한 관련 정보처리자는 해당 하위 정보처리자의 의무를 이행해야 할 책임을 상대방 당사자에 대해 부담합니다.

5.2 하위 정보처리자 목록.

Dell은 서비스 제공을 지원하기 위해 고용하는 하위 정보처리자의 목록을 www.dell.com/subprocessors에 게시합니다.

6. 보안.

6.1 기술적 및 조직적 보안 조치.

각 당사자는 개인 정보 처리에 포함되는 처리 시스템 및 서비스의 보안, 기밀성, 무결성, 가용성 및 회복탄력성이 해당 개인 정보와 관련한 위험에 상응하는지 합리적으로 확인하고 개인 정보 침해를 방지하기 위해 적절한 기술적 및 조직적 조치를 취해야 합니다. 양 당사자는 별지 1("**정보 보안 조치**")에 규정된 기술적 및 조직적 보안 조치가 개인 정보를 보호하여 이 파트너 DPA 의 요건을 충족할 수 있는 적절한 보안 수준을 제공하고 있다는 점에 동의합니다. 각 당사자는 주기적으로 (i) 안전 장치, 통제 조치, 시스템 및 절차의 유효성을 테스트 및 모니터링하고, (ii) 개인 정보의 보안, 기밀성 및 무결성에 발생할 수 있다고 합리적으로 예측 가능한 내외부 위험을 파악하고 위험이 해결되었는지 확인해야 합니다.

6.2 기술 진보.

정보 보안 조치는 해당 기술이 진보 및 발전될 수 있으며, Dell은 이에 따라 상기 조치를 수정할 수 있습니다. 다만, 수정사항이 본 계약에 따라 처리되는 개인 정보의 전체 보안 수준을 저해해서는 안 됩니다.

6.3 접근권한.

양 당사자는 개인 정보에 접근할 권한이 있는 개인(계열사 또는 승인된 하위 정보처리자 포함)이 기밀 유지 의무에 따라 개인 정보 보안 및 대외비를 준수 및 유지 관리하고 기밀 유지를 위해 노력하거나 적절한 법적 기밀 유지 의무를 준수하는지 확인해야 합니다.

7. 해외 전송.

양 당사자는 본 파트너 DPA에 따른 개인 정보 처리와 관련하여 또는 정상적인 비즈니스 과정 중에 개인 정보를 전 세계 관련 계열사 및/또는 하위 정보처리자에 전송할 수 있는 권한이 있습니다. 상기 전송을 수행할 때 각 당사자는 적절한 보호 조치를 실시하여 본 계약에 따라 또는 이에 관련하여 전송되는 개인 정보를 보호해야 합니다. 본 계약에

따라 양 당사자가 자신의 의무를 이행하는 것이 유럽 경제 지역("EEA") 또는 영국이나 스위스에서 EEA 또는 영국이나 스위스 외부의 국가(즉 개인 정보 보호법에 따른 적절성 결정의 대상이 아닌 국가)로 개인 정보를 전송하는 것을 수반하는 경우, 양 당사자는 관련 개인 정보 보호법에 따른 적절한 보완 조치 또는 기타 적절한 데이터 전송 메커니즘과 함께 모델 조항을 적용한다는 점에 동의합니다. 특히 이러한 전송 시 (a) 각 당사자는 개인 정보에 접근할 수 있는 자신의 계열사와 그룹 내부 계약을 체결하고, 해당 계약이 관련 모델 조항을 통합해야 하고, (b) 각 당사자는 관련 모델 조항을 적절하게 통합한 계약을 하위 정보처리자와 체결해야 합니다. 본 계약에 따라 양 당사자가 의무를 이행할 때 다른 국가 간의 개인 정보 전송이 수반되며 이들 국가가 관련 개인 정보 보호법에 따라 추가적으로 개인 정보 전송 관련 규정 준수 메커니즘을 하나 이상 요구하는 경우, 양 당사자는 개인 정보 보호법에서 요구하는 바에 따라 및/또는 관련 데이터 프라이버시 규제 당국에서 규정한 바에 따라 적절한 계약 조항 또는 기타 정해진 메커니즘 및/또는 수단을 사용하여 국가 간 개인 정보 전송 시 관련 규정을 준수할 것에 동의합니다.

8. 존속.

본 파트너 DPA 에 따른 각 당사자의 의무는 파트너 DPA 와의 계약이 종료된 이후에도 존속하며 개인 정보가 수신 정보통제권자의 소유이거나 통제하에 있는 한 효력이 지속됩니다.

별지 1

정보 보안 조치

Dell은 정보 보안을 중요하게 생각합니다. 본 정보 보안 개요는 Dell 그룹 계열사 간에 처리 및 전송되는 개인 정보를 보호하기 위한 Dell의 기업 관리에 적용됩니다. 임직원은 Dell의 정보 보안 프로그램을 활용하여 본인의 책임을 이해할 수 있습니다. 일부 고객 솔루션에서는 각 고객과 합의된 SOW(Statement of Work)에 대체 안전 조치를 요약할 수 있습니다.

보안 관행

Dell은 Dell의 기업 환경을 보호하고 (1) 정보 보안, (2) 시스템 및 자산 관리, (3) 개발 및 (4) 거버넌스를 해결하기 위해 고안된 회사 정보 보안 관행 및 표준을 구현했습니다. 이러한 관행과 표준은 Dell CIO의 승인을 거치며 매년 공식적으로 검토됩니다.

조직적 보안

조직의 모든 개인은 이러한 관행 및 표준을 준수할 책임이 있습니다. 회사에서 이러한 관행 및 표준을 준수하도록 촉진하기 위해 정보 보안 기능은 다음을 제공합니다.

1. 전략, 정책/표준 및 규정 준수, 인식 및 교육, 위험 평가 및 관리, 계약 보안 요구 사항 관리, 애플리케이션 및 인프라 컨설팅, 보증 검사, 회사의 보안 방향 촉진
2. 전체 환경에서 보안 관리 채택을 지원하기 위한 보안 솔루션의 보안 검사, 설계 및 구현
3. 구현된 보안 솔루션, 환경 및 자산의 보안 운영, 인시던트 대응 관리
4. 보안 운영, 법률, 데이터 보호 및 수사 인적 자원(eDiscovery 및 eForensics 포함)을 통한 포렌식 수사

자산 분류 및 관리

Dell은 물리적 및 논리적 자산을 추적하고 관리합니다. Dell IT가 추적할 수 있는 자산에는 다음이 포함됩니다.

- 정보 자산(예: 식별된 데이터베이스, 재해 복구 계획, 비즈니스 연속성 계획, 데이터 분류, 보관된 정보)
- 소프트웨어 자산(예: 식별된 애플리케이션 및 시스템 소프트웨어)
- 물리적 자산(예: 식별된 서버, 데스크탑/노트북, 백업/보관 테이프, 프린터 및 통신 장비)

자산은 대외비 요구 사항을 결정하기 위한 비즈니스의 중요성에 따라 분류됩니다. 개인 정보 처리를 위한 산업 지침은 기술적, 조직적, 물리적 보호를 위한 근거를 제공합니다. 여기에는 접근권한 관리, 암호화, 로깅 및 모니터링, 데이터 파기와 같은 제어가 포함될 수 있습니다.

개인 보안

채용 과정의 일환으로 직원은 지역 법률에 따라 해당 심사 과정을 진행합니다. Dell의 연례 규정 준수 교육에는 직원이 온라인 과정을 완료하고 정보 보안 및 데이터 프라이버시를 포함하는 평가를 통과해야 한다고 규정하는 요구 사항이 있습니다. 또한 보안 인식 프로그램에서는 특정 직무 관련 자료를 제공할 수 있습니다.

물리적/환경적 보안

Dell은 물리적 보안 프로그램에서 위험 완화와 관련하여 다양한 기술적/조직적 방법을 사용합니다. 보안 팀은 현장과 긴밀하게 협력하여 적절한 조치가 취해지고 있는지 확인하고 물리적 인프라, 비즈니스 및 알려진 위협에 대한 변경 사항을 지속적으로 모니터링합니다. 또한 업계의 다른 업체에서 사용되는 조치 모범 사례를 모니터링하고 Dell의 고유한 비즈니스 관행과 기대치를 모두 충족하는 방법을 신중하게 선택합니다. Dell은 아키텍처, 운영, 시스템을 비롯한 관리 요소를 고려하여 보안 방식을 조율합니다.

커뮤니케이션 및 운영 관리

IT 조직은 테스트, 비즈니스 영향 분석, 관리 승인을 비롯하여 적절한 중앙 집중식 변경 관리 프로그램을 통해 회사 인프라, 시스템 및 애플리케이션에 대한 변경 사항을 관리합니다.

인시던트 분석, 제약, 대응, 문제 해결, 보고, 정상 운영 복구를 비롯하여 보안 및 데이터 보호 인시던트에 대한 인시던트 대응 절차가 존재합니다.

악의적인 자산 이용과 악성 소프트웨어를 방지하기 위해 위험에 따라 추가적인 제어를 구현할 수 있습니다. 이러한 제어는 정보 보안 관행 및 표준, 제한적인 접근, 지정된 개발 및 테스트 환경, 서버/데스크탑 및 노트북의 바이러스 탐지, 바이러스 이메일 첨부 파일 검사, 시스템 규정 준수 검사, 침입 방지 모니터링 및 대응, 의심스러운 주요 이벤트에 대한 로깅 및 알림, 데이터 유형별 정보 처리 절차, 전자상거래 애플리케이션 및 네트워크 보안, 시스템 및 애플리케이션 취약성 검사를 포함하되 이에 국한되지 않습니다.

접근권한 제어

적절한 승인 확인 절차에 따라 회사 시스템에 대한 접근권한이 제한됩니다. 고의 여부를 불문하고 오용 위험을 줄이기 위해 의무와 최소한의 특권 분리에 기반하여 접근권한이 제공됩니다.

원격 접근과 무선 컴퓨팅 기능은 제한되며 사용자 보호와 시스템 보안을 모두 적용해야 합니다.

인시던트 대응 및 포렌식 수사를 지원하기 위해 예외 기준에 따라 주요 디바이스와 시스템의 특정 이벤트 로그를 중앙에서 수집하여 보고합니다.

시스템 개발 및 유지 보수

공개된 제3자 취약성이 Dell 환경에 적용 가능한지 검토합니다. Dell 비즈니스와 고객에 대한 위험에 따라 문제 해결 시간이 미리 결정됩니다. 또한 위험도에 따라 주요 신규 애플리케이션과 인프라에 대해 취약성 검사 및 평가를 실시합니다. 운영 환경으로 전환하기 전에 개발 환경에서 코드 검토와 스캐너를 사용하여 위험에 따른 코딩 취약성을 사전 예방적으로 감지합니다. 이 과정에서 취약성과 규정 준수를 사전 예방적으로 파악할 수 있습니다.

규정 준수

정보 보안, 법률, 개인 정보 보호 및 규정 준수 부서는 Dell 기업에 적용되는 지역 법률 및 규정을 파악하기 위해 노력합니다. 이러한 요구 사항에는 회사 및 고객의 지적 재산, 소프트웨어 라이선스, 직원 및 고객 개인 정보 보호, 데이터 보호, 데이터 처리 절차, 해외 데이터 전송, 재무 및 운영 절차, 기술 관련 수출 규제, 포렌식 요구 사항 등이 포함됩니다.

정보 보안 프로그램, 개인 정보 보호 운영 위원회, 내외부 감사/평가, 내외부 법률 위원회 컨설팅, 내부 제어 평가, 내부 침투 테스트 및 취약성 평가, 계약 관리, 보안 인식, 보안 컨설팅, 정책 예외 검토, 위험 관리와 같은 메커니즘을 결합하여 이러한 요구 사항 준수를 촉진합니다.

별지 2
정보 처리 설명서

1. 정보처리 대상 및 기간.

정보처리 대상 및 기간은 본 계약에 따릅니다.

2. 정보처리 목적.

개인 정보는 본 계약에 따른 의무를 이행하기 위한 목적으로 처리됩니다.

3. 정보처리의 성격.

개인 정보는 본 계약에 따른 양 당사자의 의무를 이행하는 데 필요한 경우에 처리됩니다.

4. 정보 주체의 범주.

정보 주체는 본 계약에 따른 양 당사자의 관계와 관련 있는 양 당사자의 최종 사용자, 직원, 계약업체, 공급업체 및 기타 제3자를 의미한다.

5. 개인 정보의 유형.

제출을 요청할 수 있는 개인 정보의 유형은 다음과 같습니다.

- 연락처 정보: 이름, 주소, 이메일 주소, 전화 및 기타 연락처 정보를 포함할 수 있습니다.
- 최종 고객 정보: 연락처 정보, 송장 및 신용 관련 데이터를 포함할 수 있습니다.
- IT 시스템 및 운영 정보: 개인 식별자, 음성, 동영상 및 데이터 기록, 사용자 ID 및 비밀번호 정보, 컴퓨터 이름, 이메일 주소, 도메인 이름, 사용자 이름, 비밀번호, IP 주소, 권한 데이터(직무 역할별), 통신 서비스를 위한 계정 및 위임 정보, 개인 사서함 및 디렉토리, 채팅 커뮤니케이션 데이터, 소프트웨어 및 하드웨어 인벤토리, 소프트웨어 및 인터넷 사용 패턴 관련 추적 정보(예: 쿠키), 운영 및/또는 교육 목적으로 기록된 정보를 포함할 수 있습니다.
- 정보주체의 이메일 콘텐츠 및 트래픽/전송 데이터, 온라인 대화 및 음성 통신(예: 블로그, 채팅, 웹캠, 네트워킹 세션), 지원 서비스(부수적 접근은 이메일 전송, 라우팅 및 전달과 관련한 데이터와 이메일 통신 내용에 대한 접근을 포함할 수 있음).
- 기타: 일방 당사자가 상대방 당사자에게 제출하는 모든 다른 개인 정보