3DEXPERIENCE 플랫폼
클라우드 보안 및 개인정보 보호
백서

목차

머리말

기업 철학

클라우드 컴퓨팅은 비즈니스 수행 방식 패러다임의 전환을 의미합니다. 기업은 애플리케이션을 실행하고 데이터를 관리하며 운영을 클라우드로 전환하여 클라우드 프로비저닝의 속도 및 단순성을 활용할 뿐만 아니라 전문 제공업체를 통한 유지 관리, IT 서비스 및 보안의 운영 효율성을 누리고 있습니다.

다쏘시스템은 2012년 **3D**EXPERIENCE® 플랫폼을 개발한 이래 클라우드 기반 서비스를 제공해 왔습니다. 고객이 안전하고 유연하며 확장 가능한 클라우드 리소스의 이점을 누릴 수 있는 완전한 클라우드 기반 에코시스템인 **3D**EXPERIENCE 클라우드 플랫폼을 구축했습니다. 당사는 솔루션의 모든 측면에서 신뢰와 안정성을 바탕으로 고객을 지원하는 것을 사명으로 삼고 있습니다.

위험 관리에 대한 당사의 방식은 모범 사례를 기반으로 운영 전반의 보안 위협을 예측하도록 설계된 다각적이고 사전 예방적인 방식입니다. 당사는 ISO/IEC 27001:2017 및 ISO/IEC 27701:2019 인증을 획득하고 정기적인 감사를 받는 정보 보안 및 개인정보 보호 관리 시스템(ISPMS)을 운영하고 있습니다. 당사 ISPMS는 기밀성, 무결성, 가용성, 책임성이라는 핵심 가치를 기반으로 합니다.

이 백서에서는 고객이 애플리케이션, 데이터 스토리지 및 확장 가능한 컴퓨팅 리소스에 액세스할 수 있는 클라우드 기반 플랫폼인 **3D**EXPERIENCE의 보안 및 규정 준수에 대한 다쏘시스템의 접근 방식을 간략하게 설명합니다. 이 백서에서는 클라우드 보안, 개인정보 보호 및 규정 준수 관행의 핵심적인 측면을 다룹니다.

정보 보안 및 개인정보 보호 사명

다쏘시스템 정보 보안 및 개인정보 보호 사명 선언문은 다음과 같습니다[1].

정보 보안과 위험을 관리하고 **3D**EXPERIENCE SaaS(Software as a Service)에 대한 개인 식별 정보(PII)를 보호하며 정보의 기밀성, 무결성 및 가용성을 지속적으로 개선하고 다음을 보호합니다.

- 고객 지적 재산 및 사용자 데이터, PII 포함
- 다쏘시스템의 평판 및 지적 재산
- 클라우드 가용성 및 복원력
- 사이버 보안, 데이터 보호에 해당하는 규정 및 표준 준수

이 사명 선언문은 직원에게 문서화된 정보로 제공되며, 요청 시 이해관계자에게도 제공됩니다.

책임의 한계

이 내용은 2022년 3월 기준 **3D**EXPERIENCE 클라우드 플랫폼 보안, 개인정보 보호, 품질 및 규정 준수 관행을 나타냅니다. 본 선언문에 명시된 당사 관행의 내용은 다쏘시스템의 단독 재량에 따라 변경될 수 있습니다. 이 문서 전체에서 사용되는 "당사"는 다쏘시스템을 지칭합니다.

1. ISO 27001 정보 보안 및 개인정보 처리방침에 해당합니다.

다쏘시스템: 보안과 개인정보 보호에 집중

3DEXPERIENCE 플랫폼 SAAS 사이버 보안 및 개인정보 보호

다쏘시스템 R&D는 **3D**EXPERIENCE 플랫폼 SaaS에 대해 SGS-ICS(SGS International Certification Services)에서 ISO/IEC 27001:2017 및 ISO/IEC 27701:2019 인증을 받은 중앙 제어형 정보 보안 및 개인정보 보호 관리 시스템(ISPMS)을 운영합니다. 인증 범위에는 다음이 포함됩니다.

1. **3D**EXPERIENCE 플랫폼 SaaS의 설계, 개발, 납품, 배포, 클라우드 운영 및 지원.
2. 다쏘시스템이 다음 역할을 수행하는 경우의 데이터 개인정보 보호 관리:
   - a. **3D**EXPERIENCE 플랫폼 SaaS의 맥락에서 제공되는 개인 데이터 취급 컨트롤러.
   - b. 고객이 제어하고 **3D**EXPERIENCE 플랫폼 SaaS에서 처리하는 PII 프로세서.

당사 ISPMS는 다쏘시스템 R&D 집행위원회의 관리 및 관리 검토를 받습니다. **3D**EXPERIENCE 플랫폼에서 운영되고 SGS-ICS의 ISO 9001:2015 인증을 받은 정립된 품질 관리 시스템(QMS)을 기반으로 구축되었습니다.

QMS와 ISPMS는 보안 소프트웨어 개발 생명주기(보안 SDLC) 방법론을 기반으로 하는 많은 기본 및 지원 프로세스를 공유합니다. ISPMS에는 정보 보안 및 데이터 보호에 중점을 둔 추가적인 위험 기반 프로세스도 포함되어 있습니다.

모든 ISPMS 프로세스와 제어는 다쏘시스템 R&D **3D**EXPERIENCE 규정 준수 감사 프로그램에 의해 규정 준수 및 효과성에 대한 지속적인 평가를 받습니다. 이에 따른 시정 조치와 지속적인 개선 사항은 **3D**EXPERIENCE 플랫폼 내에서 추적됩니다.

감사 기준은 ISO 9001, ISO 27001, ISO 27701 관리 시스템 및 제어 요구사항을 기반으로 합니다. 모든 ISO 27001 부록 A 제어와 ISO 27701 부록 A 및 B 제어는 관리 시스템의 범위에 포함되며, 다쏘시스템은 PII 컨트롤러 및 PII 프로세서의 역할을 모두 수행합니다(데이터 보호 및 개인정보 보호, 11 페이지 참조).

ISPMS는 **3D**EXPERIENCE 플랫폼 정보 보안 및 개인정보 보호 사명 선언문(방침 선언문)과 연간 목표의 뒷받침을 받습니다. 목표는 운영 팀이 모니터링할 수 있는 측정 가능한 세부 목표와 핵심 성과 지표(KPI)를 제시합니다. 사이버 보안 및 데이터 보호 목표는 다쏘시스템의 연간 계획 프로세스의 일부로서 그 적합성이 정기적으로 검토됩니다.

당사 보안, 개인정보 보호 및 규정 준수 담당

R&D 집행위원회

다쏘시스템 R&D 집행위원회는 데이터 보호 요구사항 및 개인정보 보호에 관해 다쏘시스템 법률 고문의 지원을 받아 **3D**EXPERIENCE 정보 보안 및 개인정보 보호 관리 시스템(ISPMS)의 효과에 대한 궁극적인 책임을 지고 있습니다. R&D 집행위원회는 다음과 같은 다양한 수단을 통해 ISPMS와 고객의 기대에 부응하기 위해 적극적으로 노력합니다.

- 정보 보안 및 개인정보 처리방침과 연간 목표가 조직의 전략적 방향과 양립할 수 있도록 합니다.
- 조직의 비즈니스 프로세스에 ISPMS 요구사항을 통합합니다.
- ISPMS에 필요한 리소스를 사용할 수 있는지 확인합니다.
- ISPMS의 중요성에 대해 소통합니다.
- ISPMS가 의도한 결과를 달성하도록 보장합니다.
- ISPMS의 효과성에 기여할 수 있도록 직원을 지휘하고 지원합니다.
- ISPMS 프로세스 및 운영의 지속적인 개선을 촉진합니다.

사이버 보안, 데이터 개인정보 보호 및 규정 준수 팀

다쏘시스템은 각 직책 또는 역할과 관련된 사명, 설명, 산출물, KPI, 역할 프로파일 및 기술을 정의하는 엔터프라이즈 역할 모델을 유지 관리합니다.

최고 정보 보안 책임자(CISO) 및 보안 리더로 구성된 팀이 다쏘시스템 정보 보안 프로그램 구현에 대한 전반적인 책임을 집니다. 이들은 글로벌 수준에서 정보 보안 방침, 표준, 가이드라인 및 절차를 수립, 유지 관리 및 시행할 책임이 있습니다.

다쏘시스템 R&D 사이버 보안 및 데이터 개인정보 보호 팀은 **3D**EXPERIENCE ISPMS가 ISO 27001 및 ISO 27701의 요구사항에 따라 계획, 구현, 유지 관리 및 지속적인 개선이 이루어지는지 확인할 책임이 있습니다. 이들은 표준 거버넌스 회의의 일환으로 ISPMS의 규정 준수 여부와 효과를 모니터링하고 이를 경영진에게 보고할 책임이 있습니다.

그룹 데이터 보호 책임자(DPO)는 모범 사례, 책임성 및 다쏘시스템의 지속 가능한 성장을 보장하기 위해 다쏘시스템에 PII 보호에 대한 정보를 제공하고 조언합니다. 그룹 DPO는 데이터 보호 감독 당국의 특권적 대화 상대이며 ISPMS의 규정 준수 및 효과에 대해 다쏘시스템의 법률 고문에게 보고합니다.

R&D 규정 준수 및 위험 팀은 내부 규정 준수 감사 프로그램을 운영하여 다쏘시스템의 내부 프로세스 및 ISO 9001, ISO 27001, ISO 27701과 같은 업계 인증 준수 여부를 평가합니다. 감사 결과와 그에 따른 시정 및 예방 조치 계획(CAPA)은 플랫폼에서 관리됩니다.

그룹 내부 감사 팀은 엔터프라이즈급 내부 감사 프로그램을 통해 다쏘시스템 내부 제어 평가(ICE) 프레임워크의 규정 준수 및 효과를 정의하고 평가합니다. 내부 제어 프레임워크는 일반 제어 및 정보 기술 일반 제어(ITGC)의 수립과 검증을 통해 위험을 완화하는 데 도움이 됩니다.

전 직원 온보딩 및 교육

다쏘시스템에 입사하는 직원은 다쏘시스템의 행동 강령, IT 헌장 및 데이터 보호 방침을 준수하는 데 동의해야 합니다. 모든 신입 직원은 다음을 포함하여 보안 및 개인정보 보호에 관한 필수 윤리 및 규정 준수 교육을 이수합니다.

- 데이터 보안에 대한 위협 방지.
- 물리적 데이터 및 워크스테이션 보안, 클린 데스크 방침.
- 개인 데이터 보호 및 기밀 유지.
- 윤리적 비즈니스 행동, 반부패 및 경쟁법 원칙.
- 인시던트 관리, 잠재적 위협 인식 및 보고.

당사는 조직 전반에 걸쳐 보안 및 개인정보 보호에 대한 인식을 지속적으로 제고하고 있습니다.

원격 근무 보안

원격 근무 시 다쏘시스템의 직원은 VPN을 통해서만 데이터, 애플리케이션, 플랫폼 유틸리티에 액세스할 수 있습니다. 이는 회사 기기와 개인 기기 모두에 적용됩니다. VPN 액세스가 가능하고, 등록되어 승인을 받은 개인 기기만 허용됩니다.

클라우드 보안 파트너

당사는 3DS Outscale을 비롯한 클라우드 인프라(IaaS) 제공업체와 긴밀히 협력하여 운영 전반의 보안 및 규정 준수를 보장합니다. 당사 IaaS 제공업체에게는 ISO 27001 및 그 외 인증을 받도록 요구합니다.

당사 보안 표준

사이버 보안에 대한 당사의 접근 방식은 가장 인정받는 업계 표준에 뿌리를 두고 있습니다. 독립된 사이버 보안 전문가들이 소프트웨어 제공업체에 대한 글로벌 표준을 수립하기 위해 적극적으로 협력하고 있습니다. OWASP, NIST, ISO/IEC는 위험을 줄이고 취약성을 완화하기 위한 모범 사례, 요구 사항, 제어, 테스트 및 기타 도구를 통해 당사 사이버 보안 및 개인정보 보호 팀을 안내하는 세 가지 전문 기관입니다.

OWASP: OPEN WEB APPLICATION SECURITY PROJECT[1]

OWASP는 조직이 매우 안전한 애플리케이션을 개발하고 유지 관리할 수 있도록 지원하는 데 전념하고 있습니다. OWASP 재단은 애플리케이션 보안과 관련된 최첨단 연구, 널리 사용되는 프레임워크 및 중요한 정보를 제공하는 대표적인 기관입니다.

글로벌 연합의 도움을 받아 OWASP는 다음을 제공합니다.

- 애플리케이션 보안 도구, 표준 및 방법론
- 보안 코드 개발, 보안 코드 검토, 애플리케이션 보안 테스트를 위한 리소스
- 표준 보안 제어 및 라이브러리

OWASP의 주요 출판물은 다음과 같습니다.

- 상위 10가지 웹 애플리케이션 보안 위험(Top 10 Web Application Security Risks)
- 시큐어 코딩 관행(Secure Coding Practices)
- 코드 검토 가이드(Code Review Guide)
- 애플리케이션 보안 검증 표준(Application Security Verification Standard)

NIST: NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY[2]

NIST는 전자, 소프트웨어 및 기타 기술 분야에서 중요한 측정 솔루션과 공정한 표준을 제공하는 탁월한 기관입니다. NIST SP(Special Publication) 800-53은 정보 시스템 및 조직에 대한 보안 제어와 개인정보 보호 제어를 정의합니다.

NIST SP 800-53은 '적대적 공격, 인적 오류, 자연재해, 구조적 장애, 외국 정보 기관, 개인정보 위험 등 다양한 위협과 위험'으로부터 조직의 운영과 자산, 개인 및 기타 단체를 보호하기 위해 설계되었습니다. 이러한 제어는 기능 및 보증 관점에서 보안 및 개인정보 보호를 다룹니다.

ISO/IEC: INTERNATIONAL ORGANIZATION FOR STANDARIZATION AND THE INTERNATIONAL ELECTROTECHNICAL COMMISION[3]

ISO/IEC는 IT 및 통신 기술 분야의 표준을 촉진하기 위해 활동하는 공동 기술 위원회입니다. **3D**EXPERIENCE 플랫폼 SaaS에 대한 당사 ISPMS는 SGS-ICS의 ISO/IEC 27001:2017 및 ISO/IEC 27701:2019 인증을 받았으며, QMS는 SGS-ICS의 ISO 9001:2015 인증을 받았습니다("**3D**EXPERIENCE 플랫폼 SaaS 사이버 보안 및 개인정보 거버넌스", 4페이지 참조).

ISO 9001은 조직이 품질 관리 시스템을 구축할 때 필요한 요구사항을 명시하고 있습니다.

a. 고객 및 관련 법률과 규제 요건을 충족하는 제품 및 서비스를 일관되게 제공할 수 있는 능력을 입증해야 합니다.

b. 시스템 개선 프로세스, 고객 및 관련 법률과 규제 요건 준수 보장을 포함한 시스템의 효과적인 적용을 통해 고객 만족도를 높이는 것을 목표로 합니다.

당사 품질 관리 시스템(QMS)은 설계, 개발, 납품, 배포, 클라우드 운영 및 **3D**EXPERIENCE 플랫폼 지원에 사용되는 프로세스에 뿌리를 두고 있습니다. 당사의 많은 애플리케이션 보안 관행이 QMS에 포함되어 있습니다.

ISO/IEC 27001은 정보 보안 관리 시스템(ISMS)을 수립, 구현, 유지 관리 및 지속적으로 개선하기 위한 요구사항을 명시합니다. ISO/IEC 27001 부록 A는 공용 네트워크에서의 애플리케이션 서비스 보안, 애플리케이션 보안 트랜잭션 보호, 보안 개발 정책 시행, 소프트웨어 패키지 변경 제한, 보안 시스템 엔지니어링 원칙 준수 등 모든 것에 대해 예상되는 제어를 명확히 설명합니다.

ISO/IEC 27701은 조직의 맥락에서 개인정보 관리를 위해 ISO/IEC 27001 및 ISO/IEC 27002를 확장한 형태로 개인정보 관리 시스템(PIMS)을 수립, 구현, 유지 관리 및 지속적으로 개선하기 위한 요구사항을 지정하고 지침을 제공합니다. 이 표준은 PII 처리의 책임과 의무를 지닌 PII 컨트롤러 및 PII 프로세서에 대한 지침을 제공합니다. 부록 A는 PII 컨트롤러에 대한 제어 목표 및 제어를 지정하고 부록 B는 PII 프로세서에 대한 제어 목표 및 제어를 지정합니다.

1. 자세히 알아보기: www.owasp.org
2. 자세히 알아보기: csrc.nist.gov
3. 자세히 알아보기: iso.org/isoiec-27001-information-security

보안 핵심 기능

인증 및 권한 부여

3DEXPERIENCE 클라우드 플랫폼의 인증 및 권한 부여 메커니즘은 사용자가 자신의 모든 역할, 앱 및 서비스에 안전하게 액세스할 수 있는 개인화된 로그인인 **3D** Passport입니다. 관리자는 암호 강도, 만료와 같은 사용자 인증 정책을 관리하고, 암호를 해제하려는 강제 시도를 감지하는 패턴을 설정합니다.

3D Passport 기능

데이터 개인정보 보호

당사 온라인 솔루션의 모든 사용자는 다쏘시스템 개인정보 처리방침에 액세스할 수 있으며 **3D** Passport 생성 시 이에 동의해야 합니다. 사용자는 웹 양식을 통해 요청을 제출하여 다쏘시스템 정책 및 절차에 따라 권리를 행사할 수 있습니다.

또한 회사가 자체 개인정보 처리방침을 사용자에게 공개하고 수락을 요구할 수도 있습니다. 이 경우 플랫폼 관리자가 플랫폼 관리 대시보드를 통해 자체 개인정보 처리방침을 업로드합니다.

SSO(Single Sign-On)

3D Passport는 인증 및 권한 부여 데이터를 표준 형식으로 교환함으로써 **3D**EXPERIENCE 클라우드 플랫폼에서 앱에 대한 완벽한 Single Sign-On 기능을 제공합니다.

MFA(Multi-Factor Authentication)

플랫폼에서 MFA 기능을 활용하면 더 높은 수준의 보안을 유지할 수 있습니다. 예를 들어, 관리자가 MFA를 구성한 후에는 보안 강화를 위해 사용자가 모바일 앱을 사용해 코드를 생성하여 암호와 함께 입력할 수 있습니다.

권한 관리

액세스 제어는 클라우드 컴퓨팅 환경에서 리소스에 액세스하거나 이를 조회 또는 사용할 수 있는 사용자를 규제합니다. 이러한 인증은 고객 데이터를 보호하고 **3D**EXPERIENCE 클라우드 플랫폼 내에서 달성할 수 있는 고객 규정 준수 및 인증 프로세스를 지원하는 데 도움이 됩니다.

암호화

전송 중인 데이터는 무결성과 기밀성을 보호하기 위해 엔드-투-엔드 HTTPS/TLS 암호화 프로토콜을 사용하여 안전하게 보호됩니다.

고가용성 및 DDOS 방지

모든 서비스는 분산 서비스 거부(DDoS) 공격 방지 및 블랙리스트 메커니즘과 통합된 고가용성, 고성능, 로드 밸런싱 프록시 서비스로 보호됩니다.

보안운영

당사 클라우드 운영

당사의 클라우드 솔루션은 3계층 구조로 구축 및 운영됩니다. 위협을 식별 및 모니터링하고 업계 표준을 사용하여 모든 계층에서 완화 조치를 수행함으로써 위험을 고려하고 우선순위를 지정합니다.

SaaS(Software as a Service)

가장 상위 계층에는 SaaS(Software as a Service) 또는 애플리케이션 계층이 있습니다. **3DEXPERIENCE** 클라우드 플랫폼 사용자가 애플리케이션에 액세스하고 이를 사용하는 곳입니다.

PaaS(Platform as a Service)

중간 계층은 PaaS(Platform as a Service) 또는 플랫폼 계층입니다. 이곳에서 당사의 **3DEXPERIENCE** 플랫폼이 구축되고 운영됩니다. 이 계층을 통해 인프라 제공업체와의 관계를 안전하게 관리하고 SaaS 계층과 상호 작용하는 데이터베이스를 저장할 수 있습니다.

PaaS 팀은 **3DEXPERIENCE** 클라우드 플랫폼을 구성하는 구성, 운영 체제, 구조 및 가상 리소스를 결정하고 클라우드 인프라 제공업체로부터 정보를 수신하는 방법을 결정합니다.

SaaS 및 PaaS 계층을 위한 중요한 위험 완화 전략에는 인증, 역할 기반 액세스 제어, 암호화, 모니터링 및 감사, DAST 및 SAST, 미들웨어 강화, 서버 강화, SSL/TLS 검사 등이 있습니다.

IaaS(Infrastructure as a Service)

IaaS(Infrastructure as a Service) 또는 인프라 계층은 당사 클라우드 컴퓨팅 리소스가 있는 곳입니다. 가상화 기능을 제공하고 백업 및 재해 복구 서비스를 유지 관리합니다.

이 계층은 다쏘시스템과 고객에게 필요에 따라 추가 처리 능력과 스토리지를 사용할 수 있는 확장성을 제공합니다.

당사의 주요 클라우드 제공업체는 다쏘시스템 그룹 회사인 3DS Outscale과 Amazon Web Services입니다.

공유 책임 모델

클라우드 컴퓨팅 모델에서 클라우드 제공업체와 클라우드 사용자는 온라인 서비스에 대해 최고 수준의 보안 및 규정 준수를 보장할 공동의 책임이 있습니다. 각 당사자에게는 클라우드 보안의 다양한 측면에 대한 책임이 있습니다.

- 클라우드 제공업체는 클라우드 인프라의 보안에 대한 책임이 있습니다.
- 플랫폼 제공업체(다쏘시스템)는 보안 구성, 관리 및 운영에 대한 책임을 집니다.
- 고객은 관리자/테넌트 관리를 포함한 애플리케이션 계층의 보안에 대한 책임이 있습니다.
- 당사는 클라우드 환경을 강화하고 운영하기 위해 CSA(Cloud Security Alliance) 및 NIST 가이드라인 외에 클라우드 제공업체의 모범 사례에 부합하는 보안 모범 사례를 따릅니다.

자세한 내용은 Outscale 모범 사례를 참조하십시오.

가용성 서비스 수준 계약(SLA)

당사의 목표는 (i) 계획된 서비스 중단 또는 (ii) 고객의 요청으로 인한 중단이 있는 경우가 아니라면 전체 시간 중 최소 99.5%의 온라인 서비스 가용성을 제공하는 것입니다.

자세한 내용은 온라인 서비스에 대한 서비스 수준 계약을 참조하십시오.

취약점 관리

취약점을 지속적으로 모니터링하고 완화하기 위한 조치의 일환으로 종합적인 위험 평가를 적용하여 위험을 식별, 분석, 평가하고, NIST SP 800-53, ISO/IEC 27001, ISO/IEC 27701에 따라 위험 처리 제어를 선택합니다.

당사는 취약점을 식별, 테스트 및 제어하기 위해 외부 및 사내 시스템을 결합하여 NIST 모범 사례에 기반한 다계층 취약점 관리 시스템을 사용합니다. 취약점 관리 시스템의 주요 부분은 네트워크 및 취약점 스캐너의 사용입니다. 수정이 필요한 취약점이 확인되면 심각도에 따라 우선순위를 지정하여 기록하고 수정이 완료될 때까지 추적합니다.

당사는 잠재적 위협에 대한 새로운 보안 조치를 지속적으로 추가하기 위해 정적 코드 분석(SAST), 동적 분석(DAST), 집중적인 수동 침투 테스트와 더불어 OWASP 모범 사례에 기반한 제어 기능을 사용합니다.

위협 감지 방법

위협 감지 방법에는 다음이 포함됩니다.

맬웨어 예방

승인되지 않은 소프트웨어의 사용을 금지하고 직원들에게 장비 사용 제한에 대해 교육합니다. 당사는 악성 코드를 식별할 수 있는 기술적 제어를 갖추고 있으며 직원 인식 교육을 실시합니다. 또한 맬웨어 인시던트 발생 시 효율적이고 신속하게 대응할 수 있는 절차를 마련했습니다.

모니터링

미들웨어, 네트워크, OS 액세스, OS를 포함한 모든 클라우드 계층에서 제어 효과와 보안 이벤트를 모니터링합니다. 자동화된 모니터링이 운영 및 기능 성능에 대한 실시간 데이터를 제공합니다.

인시던트 관리

당사는 보안 및 개인정보 보호 인시던트를 식별, 분류, 기록, 전달하는 데 체계적인 접근 방식을 사용합니다. 모든 인시던트는 연락 담당자가 당사 분류 척도에 따라 평가하며, 확립되어 있는 당사의 인시던트 관리 및 데이터 유출 프로세스를 통해 처리합니다.

애플리케이션 계층 취약점 관리

안전한 클라우드 SaaS 및 PaaS를 실행하려면 정보 통신 기술에서 흔히 발생하는 취약점을 지속적으로 식별하고 완화해야 합니다. 당사 보안 소프트웨어 개발 생명주기(보안 SDLC)의 일환으로 소프트웨어 취약성을 식별하고 기존 보안 제어를 검증하기 위한 몇 가지 주요 조치를 통합했습니다. 이러한 조치에는 다양한 개발 단계의 정적 및 동적 스캔과 광범위한 수동 침투 테스트가 포함됩니다.

정적 애플리케이션 보안 테스트(SAST)

SAST는 개발 프로세스 중에 소스 코드를 자동으로 평가하여 코드가 보안 SDLC의 다음 단계로 전달되기 전에 문제를 해결합니다. 당사는 Gartner 선정 최고의 SAST 제공업체와 협력하고 있습니다.

동적 애플리케이션 보안 테스트(DAST)

DAST는 프런트 엔드에서 아키텍처 약점과 잠재적인 보안 취약점을 자동으로 평가합니다. 당사의 DAST는 업계 최고의 보안 도구를 사용하여 수행됩니다.

수동 침투 테스트

공인된 타사 보안 전문가가 **3D**EXPERIENCE 클라우드 플랫폼 또는 특정 앱 세트에 대한 공격을 수동으로 시뮬레이션하여 보안 상태를 확인합니다.

교차 기능 품질 엔지니어링 테스트

당사의 독립된 품질 엔지니어링 팀이 위협 시나리오를 정기적으로 실행하여 보안 검증 프로세스에 기여합니다. 팀의 광범위한 제품 지식과 주요 보안 개념에 대한 강력한 수행 능력은 보안 확인 및 검증을 위한 추가 계층 역할을 합니다.

미들웨어, 네트워크 및 운영 체제 취약점 관리

당사는 여러 취약점 검사 및 자격 증명된 스캔을 통해 인터넷에 연결된 자산을 식별하고, Gartner 선정 최고의 취약점 스캐너를 사용하여 네트워크 및 자산의 잠재적인 결함을 빠르고 효율적으로 식별합니다.

패치 관리

당사는 기능 및 보안 관련 패치를 포함한 소프트웨어 업데이트를 정기적으로 적용합니다. 계획된 서비스 중단은 SLA에 명시된 대로 정기적으로 발생합니다. 또한 당사 패치 관리 및 인시던트 관리 프로세스는 계획되지 않은 서비스 중단이 가끔 발생하는 경우 몇 시간 내에 적용될 수 있는 긴급 보안 패치를 고려하고 있습니다.

보안 모니터링 및 위험 관리

당사의 종합적인 보안 모니터링 및 인시던트 관리 시스템이 보안 위협을 실시간으로 식별, 분석 및 대응합니다. 두 가지 접근 방식을 채택하여 한편으로는 취약점을 파악해 수정하고, 다른 한편으로는 보안 인시던트에 신속하게 대응합니다.

보안 모니터링

로그와 이벤트는 SIEM(Security, Incident and Event Management) 솔루션을 통해 중앙에서 수집 및 분석되며, 전담 SOC(Security Operations Center) 팀에서 연중무휴 24시간 모니터링합니다. 당사 SIEM 플랫폼은 중앙에서 데이터를 수집하고, 고급 상관관계 엔진을 사용하여 보안 이벤트를 선제적으로 식별하며, 대량의 보안 로그 데이터를 분석해 악의적인 활동 시도를 식별합니다.

3DEXPERIENCE 클라우드 플랫폼 감독 및 모니터링 서비스에는 기능, 성능 및 보안을 모니터링하기 위해 클라우드 계층 전반에 걸쳐 수십 개의 지표가 포함되어 있습니다.

사고 대응 프로세스

당사 SOC 팀은 인시던트의 성격에 따라 SIEM 솔루션에서 식별한 위험을 지속적으로 모니터링하고 평가합니다. 위험 평가를 기반으로 NIST SP 800-61 가이드라인에 따른 인시던트 관리 절차에 따라 즉시 인시던트를 처리합니다. 여기에는 봉쇄, 박멸, 복구 및 알림의 주요 단계가 포함됩니다.

패치 관리 프로세스의 일환으로 몇 시간 내에 긴급 패치가 이루어집니다(패치 관리 참조).

비즈니스 복구 계획(BCP) 및 재해 복구 계획(DRP)

비즈니스 복구 계획(BCP)과 재해 복구 계획(DRP)은 모든 클라우드 기반 소프트웨어 프로비저닝에 매우 중요합니다. 당사 BCP는 손실 시 컴퓨팅 서비스, 소프트웨어 서비스, 연결 및 데이터를 완전한 기능으로 복원하기 위한 계획을 다룹니다. DRP는 주요 사건 발생 시 손실을 제한하거나 되돌리기 위한 절차를 다룹니다.

당사는 다음을 포함하여 BCP/DRP에 대한 업계 모범 사례를 따릅니다.

1. 고객 데이터의 백업 및 복구를 위한 일관된 계획을 유지 관리하고, 대규모 재해 발생 시 모든 계획 구성 요소에 액세스할 수 있도록 합니다.

2. 중요한 데이터의 사본을 기본 데이터 센터에서 떨어진 프로덕션 지역 외부에 유지 관리합니다.

3. BCP/DRP를 최신 상태로 유지하고 프로덕션 환경의 모든 변경 사항을 고려합니다.

4. 매년 BCP/DRP를 실행합니다.

5. 로드 밸런싱 및 장애 조치 시스템과 같은 가상화 기능을 활용하여 서비스 중단을 최소화합니다.

당사는 모든 시나리오에서 고객의 비즈니스 연속성을 보장하기 위해 공격적인 복구 시간 목표(RTO)와 복구 지점 목표(RPO)에 초점을 맞추고 있습니다.

데이터 백업 및 검색

당사는 서비스 수준 계약에 의거하여 고객 및 사용자 데이터를 매일 백업하며, 이 백업은 SLA에 따라 보관됩니다. 가동 중단 시간을 최소화하고 데이터 보호를 극대화하기 위해 지속적인 핫 백업과 콜드 백업을 수행합니다.

3DEXPERIENCE 클라우드 플랫폼 고객 데이터는 SLA에 명시된 대로 정해진 기간 동안 계속 검색할 수 있습니다.

자세한 내용은 온라인 서비스에 대한 서비스 수준 계약을 참조하십시오.

데이터 및 개인정보 보호

당사 클라우드 솔루션은 고객과 사용자의 개인정보 보호를 중요하게 생각하며 구축되었습니다. 당사는 유럽 일반 개인정보 보호법(General Data Protection Regulation, GDPR) 2016/679와 같은 관련 법률 및 표준에 따라 모든 PII를 안전하게 저장하고 처리하기 위해 높은 기준을 준수합니다.

컨트롤러

GDPR에 정의된 대로 컨트롤러는 스토리지 보유기간 결정, PII 최소화 준수, 데이터 주체의 요청 처리 등 개인 데이터 취급에 대한 정책과 절차를 결정해야 합니다. 다쏘시스템은 내부 비즈니스 프로세스 및 정보 시스템과 관련된 PII를 처리할 때 컨트롤러의 역할을 수행합니다.

다쏘시스템 SaaS 솔루션의 고객은 솔루션에서 유지 관리되는 PII를 처리할 책임이 있으므로 컨트롤러의 역할을 수행합니다.

GDPR 및 기타 데이터 보호법은 개인정보 보호 권리를 확대하고 개인이 자신의 PII를 제어할 수 있도록 함으로써 거주자의 기본권을 강화하는 것을 목표로 합니다. 글로벌 기업으로서 다쏘시스템은 GDPR은 물론 다쏘시스템이 비즈니스를 수행하는 지역의 기타 데이터 보호법을 준수합니다. GDPR 및 기타 국가별 법률은 3ds.com에서 제공되는 다쏘시스템 개인정보 처리방침에서 확인할 수 있습니다.

3DEXPERIENCE 클라우드 플랫폼의 경우 다쏘시스템은 다음 사항에 대한 컨트롤러 역할을 수행합니다.

- 프라이빗 클라우드 제품을 제외한 **3D** Passport
- 3ds.com을 통해 개인이 만든 **3D** Passport
- 다쏘시스템 공개 플랫폼에서 이용 가능한 **3D**EXPERIENCE 공개 커뮤니티
- 다쏘시스템 고객 지원
- **3D**EXPERIENCE 마켓플레이스

GDPR 외에도 기타 현지 데이터 보호법 및 규정은 현지에 기반을 둔 다쏘시스템 데이터 보호 책임자가 모니터링하며, 현지 프로세스 및 절차에 따라 시행됩니다.

3D Passport는 사용자별로 생성되는 인증 프로파일입니다. **3D** Passport 내에서 PII를 처리하는 것은 다쏘시스템의 책임 하에 있습니다. **3D** Passport와 관련된 PII는 규제 요건으로 인해 일부 특정 예외를 제외하고 유럽에 저장됩니다.

프로세서

다쏘시스템이 **3D**EXPERIENCE 클라우드 플랫폼과 같은 클라우드 기반 제품을 제공하는 경우, 다쏘시스템은 처리 및 저장하도록 요청받은 PII에 대한 프로세서 역할을 수행합니다. 이러한 권한으로 다쏘시스템은 당사자 간에 체결된 계약에 따라 PII를 처리합니다.

다쏘시스템은 GDPR에 정의된 대로 다음 사항에 대해 프로세서의 역할을 수행합니다.

- 고객 및 비즈니스 파트너에게 제공된 다쏘시스템 클라우드 제품(프라이빗 및 퍼블릭)
- 프라이빗 클라우드 제품에 대한 **3D** Passport

프로세서 역할을 하는 경우 플랫폼 데이터는 현지 데이터 센터에 있는 타사 IaaS 제공업체(예: 3DS Outscale 또는 Amazon Web Services)에 저장됩니다.

맺음말

다쏘시스템은 보안과 개인정보 보호를 운영의 핵심으로 삼고 있습니다. 당사의 사이버 보안 및 데이터 보호 조치는 가장 공신력 있는 업계 표준을 기반으로 하며 교육, 설계 요건, 보안 통제, 개인정보 보호 조치, 제삼자 감사 및 테스트를 통해 체계적으로 적용됩니다. 당사는 혁신과 우수성의 정신으로 보안 및 개인정보 보호 조치를 지속적으로 개선하여 고객을 최상의 방식으로 지원할 수 있도록 노력하고 있습니다.

11개 산업부문을 지원하는 **3D**EXPERIENCE® 플랫폼은 당사의 주력 브랜드 애플리케이션으로 다양한 산업솔루션 경험을 제공하고 있습니다.

3DEXPERIENCE 기업인 다쏘시스템은 인류 발전의 기폭제입니다. 기업과 사람들이 협업할 수 있는 가상 환경을 제공하여 지속 가능한 혁신을 구상할 수 있도록 지원합니다. 당사의 고객은 **3D**EXPERIENCE 플랫폼과 애플리케이션을 통해 실제 세계의 '버추얼 익스피리언스 트윈'을 구축하여 혁신, 학습 및 생산의 저변을 넓히고 있습니다.

20,000명의 다쏘시스템 임직원들이 전 세계 140여 국가의 모든 산업 부문에서 27만 곳 이상의 고객들에게 새로운 가치를 선사하고 있습니다. 자세한 내용은 **www.3ds.com/ko**를 참고하십시오.

3DEXPERIENCE®

DASSAULT SYSTEMES | The **3D**EXPERIENCE® Company

본사
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

미주
Dassault Systèmes
175 Wyman Street
Waltham, MA 02451
USA

아시아 태평양
Dassault Systèmes
ThinkPark Tower
2-1-1 Osaki, Shinagawa-ku
Tokyo 141-6020
JAPAN