DASSAULT SYSTEMES

3DEXPERIENCE 平台
云安全和隐私
白皮书

目录

前言

我们的理念

云计算代表着我们如何开展业务的范例转换。组织正在运行应用、管理数据并将运营转移到云，以从云提供的速度和简单性中受益，并从专业提供商提供的维护、IT 服务和安全的运营效益中受益。

自 2012 年创建 **3D**EXPERIENCE® 平台以来，达索系统一直提供基于云的服务。我们构建了基于云的完整生态系统，即 **3D**EXPERIENCE 云平台，使我们的客户能够从安全、灵活、可扩展的云资源中受益。我们的宗旨是在解决方案的每个方面以信任和可靠的方式支持客户。

我们的风险管理方法是多方面且主动的，这些方法基于许多最佳实践，旨在预测我们整个运营中的安全威胁。我们运行经 ISO/IEC 27001:2017 和 ISO/IEC 27701:2019 认证的信息安全和隐私管理系统 (ISPMS)，并接受常规审计。我们的 ISPMS 基于机密性、完整性、可用性和责任制等核心价值观。

本白皮书概述达索系统基于云的平台 **3D**EXPERIENCE 安全和合规性的方法，客户可在此平台上访问应用、数据存储和可扩展的计算资源。在本白皮书中，我们讨论云安全、隐私和合规做法的核心方面。

我们的信息安全和隐私宗旨声明

达索系统信息安全和隐私宗旨声明如下 [1]。

管理信息安全风险暴露并保护 **3D**EXPERIENCE 平台软件即服务 (SaaS) 的个人可识别信息 (PII)，同时不断提高信息的机密性、完整性和可用性，并保护以下内容：

- 客户知识产权和用户数据，包括 PII
- 达索系统的声誉和知识产权
- 云可用性和弹性
- 遵守适用的网络安全和数据保护法规和标准

本宗旨声明可作为书面信息提供给员工，也可根据要求提供给利益相关方。

免责声明

此内容代表着截至 2022 年 3 月的 **3D**EXPERIENCE 云平台安全、隐私、质量和合规做法。此处列出的做法内容由达索系统自行决定是否更改。本文档使用的"我们"和"我们的"专门

1.这与 ISO 27001 信息安全和隐私政策相对应。

指达索系统。

达索系统：专注于安全和隐私的组织

3DEXPERIENCE 平台 SaaS 网络安全和隐私管理

达索系统研发运营着 **3D**EXPERIENCE 平台 SaaS 集中控制的信息安全和隐私管理系统 (ISPMS)，其经 ISO/IEC 27001:2017 和 ISO/IEC 27701:2019 的 SGS 国际认证服务 (SGS-ICS) 认证。认证范围包括：

1. **3D**EXPERIENCE 平台 SaaS 的设计、开发、交付、部署、云运营和支持。
2. 达索系统在充当以下角色时的数据隐私管理：
   - **a.** 控制器，用于处理在 **3D**EXPERIENCE 平台 SaaS 上下文中提供的个人数据。
   - **b.** PII 处理器，由客户控制并在 **3D**EXPERIENCE 平台 SaaS 中进行处理。

我们的 ISPMS 由达索系统研发执行委员会管理并接受管理审查。此系统建立在成熟的质量管理体系 (QMS) 之上，在 **3D**EXPERIENCE 平台上运行，并经 SGS-ICS 认证，符合 ISO 9001:2015 标准。

QMS 和 ISPMS 共享许多基于安全软件开发生命周期 (Secure SDLC) 方法的基本和支持流程。ISPMS 还包括其他以信息安全和数据保护为中心的基于风险的流程。

达索系统研发 **3D**EXPERIENCE 合规性审计计划会持续评估所有 ISPMS 流程和控制的合规性和有效性。在 **3D**EXPERIENCE 平台中跟踪产生的纠正措施和持续改进。

审核标准基于 ISO 9001、ISO 27001 和 ISO 27701 管理系统和控制要求。所有 ISO 27001 附件 A 控制以及 ISO 27701 附件 A 和 B 控制均包含在管理系统的范围内，因为达索系统同时充当 PII 控制器和 PII 处理器的角色（请参阅"数据保护和隐私"，第 11 页）。

ISPMS 受到 **3D**EXPERIENCE 平台信息安全和隐私宗旨声明（政策声明）和年度目标的支持。目标提供可衡量的目标和关键绩效指标 (KPI)，由运营团队监控。定期审查网络安全和数据保护目标的适合度，这是达索系统年度规划流程的一部分。

我们的安全、隐私和合规人员

研发执行委员会

在达索系统总顾问的支持下，达索系统研发执行委员会最终负责 **3D**EXPERIENCE 信息安全和隐私管理系统 (ISPMS) 的有效性，以满足数据保护要求和隐私。研发执行委员会通过各种方式积极展示其对 ISPMS 和客户期望作出的承诺，包括：

- 确保信息安全和隐私政策及年度目标与组织的战略方向一致；
- 确保将 ISPMS 要求纳入组织的业务流程；
- 确保 ISPMS 所需的资源可用；
- 传达 ISPMS 的重要性；
- 确保 ISPMS 达到预期结果；
- 指导和支持人员为提高 ISPMS 的有效性做出贡献；
- 促进 ISPMS 流程和运营的持续改进。

网络安全、数据隐私和合规团队

达索系统维持企业角色模型，该模型可定义与每个职位或角色相关的任务、描述、交付成果、KPI、职责介绍和技能。

首席信息安全官 (CISO) 和安全负责人团队全面负责实施达索系统信息安全计划。他们负责在全球层面制定、维护和实施信息安全政策、标准、准则和程序。

根据 ISO 27001 和 ISO 27701 的要求，达索系统研发网络安全和数据隐私部门负责确保计划、实施、维护和持续改进 **3D**EXPERIENCE ISPMS。他们负责监控 ISPMS 的合规性和有效性，并将此内容作为标准治理会议的一部分向高管汇报。

集团数据保护专员 (DPO) 向达索系统提供有关 PII 保护的信息和建议，以确保最佳做法、问责制和达索系统的可持续发

展。集团 DPO 是数据保护监管机构的特许对话者，向达索系统总顾问报告 ISPMS 的合规性和有效性。

研发合规与风险团队运行内部合规性审计计划，以评估达索系统对内部流程和行业认证（如 ISO 9001、ISO 27001 和 ISO 27701）的合规情况。在平台中管理审计结果和相应的纠正和预防措施规划 (CAPA)。

集团内部审计团队通过企业级内部审计计划定义并评估达索系统内部控制评估 (ICE) 框架的合规性和有效性。内部控制框架通过建立和验证一般控制和信息技术一般控制 (ITGC) 帮助降低风险。

所有员工的入职和培训

加入达索系统的员工必须同意遵守我们的行为准则、IT 章程和数据保护政策。所有新员工均必须接受涉及安全和隐私的道德和合规性培训，包括：

- 防止数据安全威胁。
- 确保实际数据和工作站的安全；清理办公桌政策。
- 个人数据保护和保密。
- 商业道德行为；反腐败和竞争法原则。
- 事件管理；识别和报告潜在威胁。

我们在整个组织内不断促进安全和隐私意识培养。

远程工作的安全

达索系统员工在远程工作时，只能通过 VPN 访问其数据、应用和平台实用。这适用于公司和个人设备。仅允许具有 VPN 访问权限的已注册和已批准的个人设备。

我们的云安全合作伙伴

我们与云基础设施 (IaaS) 提供商（包括 3DS Outscale）密切合作，以确保整个运营的安全性和合规性。除其他标准外，我们要求 IaaS 提供商要经 ISO 27001 认证。

我们的安全标准

我们的网络安全方法扎根于最受尊重的行业标准。独立的网络安全专家们积极协作，为软件提供商建立全球标准。OWASP、NIST 和 ISO/IEC 是三所专家机构，通过最佳做法、要求、控制、测试和其他工具来指导我们的网络安全和隐私团队，以降低风险和减少漏洞。

OWASP：开放式 WEB 应用安全项目 [1]

OWASP 致力于使组织能够开发和维护高度安全的应用。OWASP Foundation 是与应用安全相关的前沿研究、普遍框架和重要信息的主要来源。

在全球联盟的帮助下，OWASP 提供：

- 应用安全工具、标准和方法
- 用于安全代码开发、安全代码审查和应用安全测试的资源
- 标准安全控制和库

OWASP 的主要出版物包括：

- 10 大 Web 应用安全风险
- 安全编码做法
- 代码审查指南
- 应用安全验证标准

NIST：国家标准和技术研究院[2]

NIST 是关键测量解决方案和电子、软件和其他技术的公平标准的卓越来源。NIST 特殊出版物 (SP) 800-53 定义信息系统和组织的安全控制和隐私控制。

NIST SP 800-53 旨在保护组织运营和资产、个人和其他实体免受"各种威胁和风险，包括恶意攻击、人为错误、自然灾

害、结构故障、外国智能实体和隐私风险。"这些控制从功能和保证角度解决安全和隐私问题。

ISO/IEC：国际标准化组织和国际电工委员会 [3]

ISO/IEC 是一个联合技术委员会，致力于促进 IT 和通信技术标准。我们的 **3D**EXPERIENCE 平台 SaaS 的 ISPMS 经 ISO/IEC 27001:2017 和 ISO/IEC 27701:2019 认证，而我们的 QMS 经 ISO 9001:2015 认证，两者均由 SGS-ICS 认证（请参阅"**3D**EXPERIENCE 平台 SaaS 网络安全和隐私管理"，第 4 页）。

ISO 9001 在组织处于以下情况时指定对质量管理体系的要求：

a. 需要展示其能够始终如一地提供符合客户及适用的法定和法规要求的产品和服务，及

b. 旨在通过系统的有效应用提升客户满意度，包括改进系统流程、确保符合客户要求和适用的法定和法规要求。

我们的质量管理体系 (QMS) 扎根于用于设计、开发、交付、部署、云运营的流程，同时支持 **3D**EXPERIENCE 平台。我们将许多应用安全做法嵌入到 QMS 中。

ISO/IEC 27001 指定建立、实施、维护和持续改进信息安全管理系统 (ISMS) 的要求。ISO/IEC 27001 附件 A 清晰描述从确保公共网络上的应用服务安全、保护应用安全事务、强制实施安全开发策略、限制更改软件包、遵守安全系统工程原则等所有方面的预期控制。

ISO/IEC 27701 以 ISO/IEC 27001 和 ISO/IEC 27002 的扩展形式，指定建立、实施、维护和持续改进隐私信息管理系统 (PIMS) 的要求并提供指导，以实现组织上下文中的隐私管理。这一标准为负责 PII 处理的 PII 控制器和 PII 处理器提供指导。附件 A 指定 PII 控制器的控制目标和控制措施，附件 B 指定 PII 处理器的控制目标和控制措施。

1.了解更多信息：www.owasp.org
2.了解更多信息：csrc.nist.gov
3.了解更多信息：iso.org/isoiec-27001-information-security

关键安全功能

身份验证和授权

3DEXPERIENCE 云平台的身份验证和授权机制是 **3D** Passport，这是一种个性化登录，允许用户安全访问所有角色、应用和服务。管理员可以维护用户身份验证政策（比如密码的强度、过期和配置模式），以便检测暴力破解解锁密码的尝试。

3D Passport 功能

数据隐私

使用在线解决方案的每位用户都可以访问达索系统隐私政策，并且在创建 **3D** Passport 时需要接受该政策。用户可以通过 Web 表单提交请求，根据达索系统政策和流程行使其权利。

此外，公司还可以向用户提供隐私政策供其接受。在这种情况下，平台管理员通过平台管理仪表板上传自己的隐私政策。

单点登录 (SSO)

通过以标准格式交换身份验证和授权数据，**3D** Passport 在 **3D**EXPERIENCE 云平台上的应用之间提供无缝的单点登录体验。

多因素身份验证 (MFA)

通过在平台上使用 MFA 功能，可以实现更高级别的安全性。例如，在管理员配置 MFA 后，用户就可以使用移动应用程序生成要输入的代码和密码，以提高安全性。

访问控制

访问控制可在我们的云计算环境中规定可以访问、查看或使用资源的人。这些授权有助于保护客户数据的安全，并支持在**3D**EXPERIENCE 云平台中可实现的客户合规和认证流程。

加密

传输过程中的数据使用端到端 HTTPS/TLS 加密协议来保护完整性和机密性。

高可用性和反 DDOS

所有服务均受到高可用性、高性能、负载平衡代理服务的保护，该服务与反 DDoS（分布式受拒服务）攻击和黑名单机制相集成。

运营安全

我们的云运营

我们的云解决方案在三层结构上构建和运营。我们使用行业标准识别和监控威胁，并在每一层执行缓解措施，以考虑并优先考虑风险。

软件即服务 (SaaS)

最高层是软件即服务 (SaaS) 或应用层。这就是 **3D**EXPERIENCE 云平台用户访问和使用其应用的位置。

平台即服务 (PaaS)

中间层是平台即服务 (PaaS) 或平台层。这就是 **3D**EXPERIENCE 平台构建和运营的位置。这一层允许我们安全地管理与基础设施提供商的关系，并存储 SaaS 层与之进行交互的数据库。

我们的 PaaS 团队确定构成 **3D**EXPERIENCE 云平台的配置、操作系统、结构和虚拟资源，并确定我们如何接收云基础设施提供商提供的信息。

SaaS 和 PaaS 层的关键风险缓解策略包括身份验证、基于角色的访问控制、加密、监控和审计、DAST 和 SAST、中间件强化、服务器强化和 SSL/TLS 检查。

基础设施即服务 (IaaS)

基础设施即服务 (IaaS) 或基础设施层是我们的云计算资源所在的位置。它们提供虚拟化功能并维护备份和灾难恢复服务。

这一层可为达索系统和我们的客户提供可扩展性，并按需提供其他的处理能力和存储。

我们主要的云提供商是 3DS Outscale（达索系统集团的一家公司）和 Amazon Web Services。

共担责任模式

在云计算模型中，云提供商和云用户共担责任以确保在线服务的最高安全和合规性级别。各方对云安全的不同方面负责：

- 云提供商负责云基础设施的安全。
- 平台提供商（达索系统）负责安全配置、管理和运营。
- 客户负责应用层的安全，包括管理员/租户管理。
- 除 CSA（云安全联盟）和 NIST 准则外，我们还按照云提供商的最佳做法，遵循安全最佳做法来强化和运营云环境。

有关详细信息，请参阅 Outscale 最佳做法。

可用性 SLA （服务水平协议）

我们的目标是在至少 99.5% 的时间内提供我们的在线服务，其中在线服务时间不在 (i) 计划服务中断或 (ii) 客户请求导致的中断内。

有关详细信息，请参阅我们的 在线服务的服务水平协议。

漏洞管理

作为我们持续监控和减少漏洞措施的一部分，我们应用全面风险评估来识别、分析和评估风险，并根据 NIST SP 800-53、ISO/IEC 27001 和 ISO/IEC 27701 选择风险处理控制。

我们采用基于 NIST 最佳做法的多层漏洞管理系统，将外部系统和内部系统相结合，以识别、测试和控制漏洞。我们漏洞管理系统的主要部分是使用网络和漏洞扫描器。如果识别到需要修复的漏洞，系统会进行记录，并根据严重程度优先考虑漏洞，然后跟踪，直至其得以修复。

我们使用静态代码分析 (SAST)、动态分析 (DAST) 和大量的手动渗透测试和基于 OWASP 最佳做法的控制，不断增加针对潜在威胁的新安全措施。

威胁检测方法

我们的威胁检测方法包括：

恶意软件预防

我们禁止使用未经授权的软件，并就设备的可接受使用培训员工。我们拥有识别恶意代码的技术控制，并开展员工意识培训。此外，我们制定了相关程序，以确保在发生恶意软件事件时能够快速有效地做出响应。

监控

我们监控所有云层（包括中间件、网络、操作系统访问和操作系统）的控制有效性和安全事件。自动监测提供有关运营和功能性能的实时数据。

事件管理

我们采用系统化的方法来识别、分类、记录和交流安全和隐私事件。所有事件均由联络点根据我们的类别规模评估，并通过我们已建立的事件管理和数据泄露流程处理。

应用层漏洞管理

运行安全的云 SaaS 和 PaaS 需要持续识别和减少漏洞，而这些漏洞在信息和通信技术中很常见。作为安全软件开发生命周期 (Secure SDLC) 的一部分，我们集成了多种关键措施来识别软件漏洞并验证我们现有的安全控制。这些措施包括在各个开发阶段进行静态和动态扫描以及广泛的手动渗透测试。

静态应用安全测试 (SAST)

SAST 在开发过程中自动评估源代码，以在代码传递到 Secure SDLC 的下一阶段之前修复问题。我们与 Gartner 领先的 SAST 提供商合作。

动态应用安全测试 (DAST)

DAST 通过前端自动评估平台的架构弱点和潜在安全漏洞。我们使用领先的行业安全工具执行 DAST。

手动渗透测试

经授权的第三方安全专业人员会手动模拟 **3D**EXPERIENCE 云平台或特定应用集上的攻击，以确认其安全态势。

跨职能质量工程测试

我们的独立质量工程团队通过例行运行威胁情形，为安全验证流程做出贡献。他们广泛的产品知识和对关键安全概念的强大命令充当安全验证和确认的额外层。

中间件、网络和操作系统漏洞管理

我们使用多种漏洞检查和有资质的扫描来识别面向网络的资产，使用 Gartner 领先的漏洞扫描器快速高效地识别我们网络和资产中的潜在缺陷。

修补程序管理

我们会定期应用软件更新，包括功能和安全相关的修补程序。计划服务中断会按照 SLA 中的设定定期发生。此外，我们的修补程序管理和事件管理流程还考虑了可在数小时内应用的紧急安全修补程序，这会产生偶尔的计划外服务中断。

安全监控和事件管理

我们全面的安全监控和事件管理系统可实时识别、分析和响应安全威胁。我们采取双管齐下的方法，一方面识别和修复漏洞，另一方面快速响应安全事件。

安全监控

日志和事件通过我们的 SIEM（安全、事件和事件管理）解决方案集中收集和分析，并由我们的专业 SOC（安全运营中心）团队全天候监控。我们的 SIEM 平台集中收集数据，并使用高级关联引擎主动识别安全事件，分析大量安全日志数据以识别恶意活动企图。

我们的 **3D**EXPERIENCE 云平台监管和监控服务包括跨云层的数十个指标来监控功能、性能和安全。

事件响应流程

我们的 SOC 团队根据事件的性质持续监控和评估 SIEM 解决方案识别到的风险。我们根据风险评估，按照 NIST SP 800-61 准则的事件管理程序，立即处理事件。这包括拦截、消除、恢复和通知的主要阶段。

作为修补程序管理流程的一部分，紧急修补程序在数小时内完成（请参阅"修补程序管理"）。

业务恢复计划 (BCP) 和灾难恢复计划 (DRP)

业务恢复计划 (BCP) 和灾难恢复计划 (DRP) 对于任何基于云的软件提供都至关重要。我们的 BCP 可解决在损失发生时将计算服务、软件服务、连接和数据恢复到完整功能的计划。我们的 DRP 可解决在发生重大事件时限制或逆转损失的程序。

我们遵循 BCP/DRP 的行业最佳做法，包括：

1.维护客户数据备份和恢复的一致计划，并确保在发生重大灾难时可访问所有计划组成部分。

2.在远离主要数据中心的生产区域之外维护关键数据的副本。

3.保持我们的 BCP/DRP 最新，并确保考虑生产环境的任何变化。

4.每年执行我们的 BCP/DRP。

5.利用虚拟化功能（如负载平衡和故障切换系统）确保将服务中断降至最低。

我们的目标是制定积极的恢复时间目标 (RTO) 和恢复点目标 (RPO)，以确保客户在所有情形下的业务连续性。

数据备份和检索

根据服务水平协议，我们确保每日备份客户和用户数据，并根据 SLA 留存。我们执行连续的热备份和冷备份，实现最大程度地减少停机时间，同时最大限度地保护数据。

3DEXPERIENCE 云平台客户数据在 SLA 中指定的一段时间内仍可供检索。

有关详细信息，请参阅我们的在线服务的服务水平协议。

数据保护和隐私

我们的云解决方案是在尊重客户和用户隐私的基础上构建的。我们遵循高标准，以确保所有 PII 按照相关法律和标准得到安全的存储和处理，例如欧洲通用数据保护条例 2016/679 (GDPR)。

控制器

根据 GDPR 的定义，控制器需要确定处理个人数据的政策和程序，包括确定存储保留期，遵守 PII 最小化和处理数据主体的请求。达索系统在处理与其内部业务流程和信息系统相关的 PII 时充当控制器的角色。

达索系统 SaaS 解决方案的客户负责处理解决方案中维护的 PII，因此充当控制器的角色。

GDPR 和其他数据保护法旨在通过扩大隐私权利并让个人能够控制 PII 来加强公民的基本权利。作为一家全球公司，达索系统遵守 GDPR 和达索系统开展业务地点所适用的其他数据保护法。达索系统隐私政策可在 3ds.com 上找到，其中引用了 GDPR 和其他特定国家/地区的法律。

对于 **3D**EXPERIENCE 云平台，达索系统充当以下的控制器角色：

- **3D** Passport（私有云产品除外）
- 由个人创建通过 3ds.com 创建的**3D** Passport
- 达索系统公共平台上提供的 **3D**EXPERIENCE 公共社区
- 达索系统客户支持
- **3D**EXPERIENCE Marketplace

除了 GDPR 之外，其他本地数据保护法律和法规由基于区域的达索系统数据保护专员监控，并由当地流程和程序实施。

3D Passport 是每个用户创建的身份验证配置文件。在 **3D** Passport 中处理的 PII 由达索系统负责。由于法规要求，与 **3D** Passport 关联的 PII 存储在欧洲（有一些特定的例外情况）。

处理器

在达索系统提供基于云的产品时（例如 **3D**EXPERIENCE 云平台），其充当要求处理和存储的 PII 的处理器。达索系统以此身份根据双方签署的合同协议处理 PII。

达索系统充当 GDPR 定义的处理器角色，具体如下：

- 达索系统（私有云和公共云）提供给客户和业务合作伙伴的云产品
- 私有云产品的 **3D** Passport

在充当处理器时，平台数据将由第三方 IaaS 提供商（例如 3DS Outscale 或 Amazon Web Services）存储在本地数据中心。

结语

达索系统将安全和隐私置于其运营的核心。我们的网络安全和数据保护措施基于非常知名的行业标准，并通过培训、设计要求、安全控制、隐私措施以及第三方审计和测试进行系统地应用。我们以创新和卓越的精神不断改进我们的安全和隐私措施，确保我们以尽可能理想的方式支持客户。

我们的 3DEXPERIENCE® 平台为我们服务于 11 个行业领域的品牌应用程序提供了技术驱动，同时提供了一系列丰富的行业解决方案经验。

3DEXPERIENCE 公司达索系统是人类进步的催化剂。我们为企业和用户提供可持续构想创新产品的虚拟协作环境。借助我们的 **3DEXPERIENCE** 平台和应用程序，我们的客户能够打造真实世界的"孪生虚拟体验"，从而拓展了创新、学习和生产的边界。

达索系统的 20,000 名员工为 140 多个国家/地区、各行各业、不同规模的 270,000 多家客户带来价值。更多信息，请访问 **www.3ds.com/zh**。

3DEXPERIENCE®

DASSAULT SYSTEMES | The 3DEXPERIENCE® Company

公司总部
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
法国

美洲
Dassault Systèmes
175 Wyman Street
Waltham, MA 02451
USA

亚太地区
Dassault Systèmes
ThinkPark Tower
2-1-1 Osaki, Shinagawa-ku
东京 141-6020
日本