DASSAULT SYSTEMES

SECURITY BY DESIGN

The **3D**EXPERIENCE® Platform Application Security Program

EXECUTIVE SUMMARY

With the growth of web-based technologies and cloud services comes a shift in responsibility for security. Organizations and individuals are increasingly dependent on application development teams to protect data and ensure privacy.

As a global leader in 3D modeling, simulation, collaboration, innovation and business intelligence software, we continuously invest in a comprehensive information security program for our **3D**EXPERIENCE platform and applications.

Our approach to information security is grounded in industry-leading practices and standards from OWASP, NIST and ISO. We apply these standards methodically through our culture of security, a Secure Software Development Life Cycle (Secure SDLC) and essential controls such as multi-factor authentication (MFA), audit trails, encryption and more.

Unique to our approach to application security is how we have integrated the verification and validation of security standards into our centrally managed **3D**EXPERIENCE Quality Management System (QMS).

Finally, frequent cycles of comprehensive internal compliance audits, third-party audits and penetration tests reinforce our stringent efforts to minimize risks and protect our customers.

This paper offers a closer look at the guidelines, processes, tools and controls that comprise the **3D**EXPERIENCE Platform Application Security Program.

CYBERSECURITY INDUSTRY STANDARDS

Our approach to application security is rooted in the most respected industry standards. Independent cybersecurity experts actively collaborate to establish global standards for all software providers. OWASP, NIST and ISO/IEC are three such standards bodies that equip developers with best practices, requirements, tests and other tools for understanding and removing vulnerabilities from enterprise software and IT systems.

OWASP

OWASP: Open Web Application Security Project

OWASP is dedicated to enabling organizations to develop and maintain highly secure applications. The OWASP Foundation is the leading source for cutting-edge research, prevalent frameworks and vital information related to application security.

With the help of global alliances, OWASP provides:

- Application security tools, standards and methodologies
- Resources for application security testing, secure code development and secure code reviews
- Standard security controls and libraries

OWASP's major publications[1] include:

- Top 10 Web Application Security Risks
- Secure Coding Practices
- Code Review Guide
- Application Security Verification Standard

[1] *Learn more at www.owasp.org*

NIST: National Institute of Standards and Technology

NIST is the preeminent source for critical measurement solutions and equitable standards in electronics, software and other technologies. NIST Special Publication (SP) 800-53 defines security controls and privacy controls for information systems and organizations.

NIST SP 800-53 is designed to protect organizational operations and assets, individuals, and other entities from "a diverse set of threats and risks, including hostile attacks, human errors, natural disasters, structural failures, foreign intelligence entities, and privacy risks."[2] These controls address security and privacy from both functionality and assurance perspectives.

ISO/IEC: International Organization for Standardization and the International Electrotechnical Commission

ISO/IEC is a joint technical committee that works to promote standards in IT and communications technology. The ISO/IEC 27001 standard[3] provides requirements for establishing, implementing, maintaining and continually improving an information security management system.

ISO/IEC 27001 Annex A articulates the expected controls for everything from securing application services on public networks, protecting application security transactions, enforcing a secure development policy, restricting changes to software packages, abiding by secure system engineering principles, and so on.

THE 5 PILLARS OF THE 3DEXPERIENCE PLATFORM APPLICATION SECURITY PROGRAM

We implement the security practices endorsed by OWASP, NIST, ISO/IEC and other organizations, plus our self-imposed protocols, through a formal governance strategy: The **3D**EXPERIENCE Platform Application Security Program.

This Security Program ensures we methodically apply the most effective security processes and tools for a Secure Software Development Lifecycle (Secure SDLC). We constantly measure and improve upon the Security Program in accordance with our Quality Management System (QMS) and its corresponding ISO 9001 certification.

Therefore, based on industry standards, Secure SDLC processes and continuous improvement, the **3D**EXPERIENCE Platform Application Security Program consists of 5 pillars:

1. **Training and Security Culture**
2. **Security Requirements and Secure Design**
3. **Implementation of Security Controls**
4. **Verification of Security Controls**
5. **Third-Party Security Audits and Penetration Testing**

[2] *Learn More: csrc.nist.gov*
[3] *Learn More: iso.org/isoiec-27001-information-security*

PILLAR 1. TRAINING AND SECURITY CULTURE

As part of the Dassault Systèmes onboarding process, all employees are trained on ethics, security and compliance protocols, and continuous improvement principles. We run ongoing awareness and communication programs for all employees to adapt to a changing security landscape.

Specific roles such as software developers, quality assurance (QA) engineers and cloud reliability engineers receive specialized training to develop a technical proficiency around relevant security threats, mitigating controls and root cause analysis.

Technical training programs emphasize countermeasures against OWASP's Top 10 Web Application Security Risks. Topics account for SQL injection, parameter tampering, command injection, XSS, CSRF, XXE and more.

We also actively collaborate with local OWASP chapters in various regions to exchange insights on the most current risk mitigation strategies.

PILLAR 2. SECURITY REQUIREMENTS AND SECURE DESIGN

Security controls are embedded throughout our SDLC, starting with the requirements phase and retained through deployment and maintenance. Security specifications are determined as part of software development projects from the start.

We build our information security procedures and controls based on the Confidentiality, Integrity and Availability (CIA) Model, also known as the CIA Triad.

Confidentiality

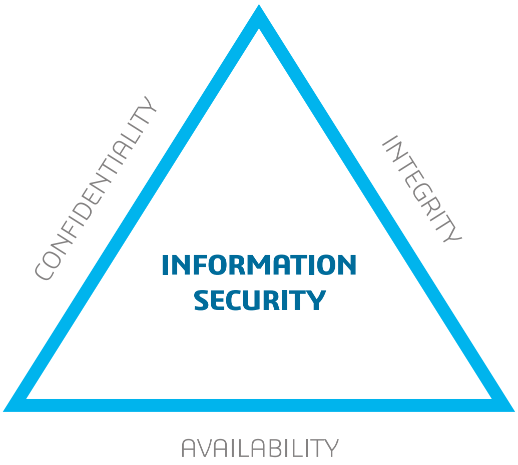
Information is protected from unauthorized access and misuse.

Integrity

Data is reliable, correct and protected from unauthorized changes.

Availability

Authorized users can access what they need when they need it.



Through risk analysis, we identify and prioritize potential security threats. We model factors such as criticality and impact to implement mitigation tactics and interventions across each stage of the Secure SDLC.

PILLAR 3. IMPLEMENTATION OF SECURITY CONTROLS

We align with NIST SP 800-53 and ISO/IEC 27001 to deliver critical security features, including authentication, access control, encryption, injection detection and prevention, auditing and server hardening.

Key security controls of the **3D**EXPERIENCE platform include:

Authentication

3DPassport supports SAML integration while providing authentication and authorization services within the platform. Multi-factor authentication and strong password policies defend against brute force attacks, privilege escalations and session hijacking. Authenticated users are assigned specific licenses and policies. Events and actions are traceable. Certificates are managed by a certificate authority and keystores.

Role-based Access Control

Access to data is restricted by organization and role-based access lists. Only authorized users can access data stored on the platform. Authorization is implemented through business logic and database layers, ensuring data integrity and strict confidentiality throughout the data lifecycle.

Encryption

Transport Layer Security (TLS) encryption protects the privacy and integrity of data in transit. Files are exchanged via a secure network connection using HTTPS/TLS to prevent man-in-the-middle attacks, eavesdropping and tampering.

Monitoring and Auditing

Automated monitoring provides real-time data on operational and functional performance. Events, actions and activities executed within the platform are logged and retained to create an audit trail and allow for investigative actions if needed.

Infrastructure Security

The **3D**EXPERIENCE platform and applications are hosted by secure infrastructure service providers certified to ISO 27001 and other security and data privacy standards. Operating systems, servers and software are hardened, patched and kept current. Communications with the platform are filtered and segmented by firewalls and the network is monitored 24/7/365.

PILLAR 4. VERIFICATION OF SECURITY CONTROLS

Before deployment, we verify that our software avoids introducing new vulnerabilities or undermining existing security controls. We run multiple simulations to test the quality of both functionality and security measures.

Primary application security analysis tools include:

Static Application Security Testing (SAST)

SAST automatically assesses the source code during the development process to fix issues before the code is passed to the next phase of the Secure SDLC.

Dynamic Application Security Testing (DAST)

DAST automatically assesses the platform through the front end for architectural weaknesses and potential security vulnerabilities.

Manual Penetration Testing

Authorized security professionals manually simulate attacks on the platform or specific set of apps to confirm their security posture.

Cross-Functional QA Testing

Our independent QA engineering teams contribute to the security verification process by routinely running various threat scenarios. Their extensive product knowledge and strong command of key security concepts serve as an extra layer of security verification and validation.

PILLAR 5. THIRD-PARTY SECURITY AUDITS AND PENETRATION TESTING

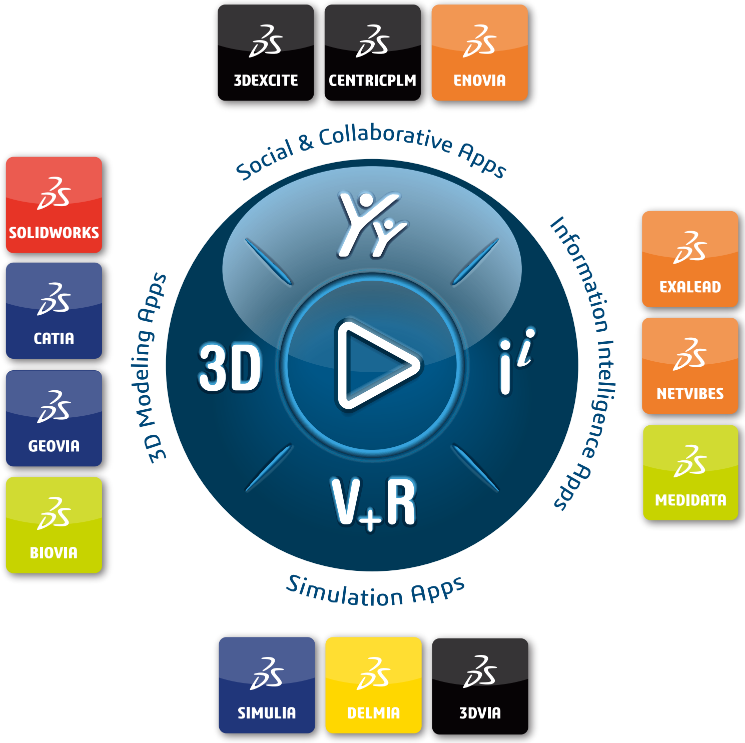
Finally, we commission independent agents with industry-leading security certifications to perform comprehensive audits and penetration tests. These confidential partners are given full access to the back-end source code and end-to-end communications for a transparent, white-box approach to test the platform down to its internal structures.

Spontaneous and scheduled tests are run multiple times per year (on average with every Service Pack released to clients) to support a continuous delivery service strategy.

CONCLUSION

Security is paramount for any application exposed to the internet today. The security industry's best practices from independent organizations including OWASP, NIST and ISO are the basis for our defensive system. Such guidelines and frameworks are systematically applied to our Secure SDLC through training, design requirements, implementation of security controls, verification of security controls, and third-party audits and penetration testing.

The **3D**EXPERIENCE Platform Application Security Program systematically mitigates risks posed by existing and future threats, safeguards data and produces the highest level of protection for customers and users.



Our **3D**EXPERIENCE® platform powers our brand applications, serving 11 industries, and provides a rich portfolio of industry solution experiences.

Dassault Systèmes, the **3D**EXPERIENCE Company, is a catalyst for human progress. We provide business and people with collaborative virtual environments to imagine sustainable innovations. By creating 'virtual experience twins' of the real world with our **3D**EXPERIENCE platform and applications, our customers push the boundaries of innovation, learning and production.

Dassault Systèmes' 20,000 employees are bringing value to more than 270,000 customers of all sizes, in all industries, in more than 140 countries. For more information, visit **www.3ds.com**.

Europe/Middle East/Africa
Dassault Systèmes
10, rue Marcel Dassault
CS 40501
78946 Vélizy-Villacoublay Cedex
France

Asia-Pacific
Dassault Systèmes K.K.
ThinkPark Tower
2-1-1 Osaki, Shinagawa-ku,
Tokyo 141-6020
Japan

Americas
Dassault Systèmes
175 Wyman Street
Waltham, Massachusetts
02451-1223
USA

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