DORA Compliance & Security Statement

Oxygen XML Editor

Product Name: Oxygen XML Editor Suite

Deployment Model: On-Premise / Standalone

Provider: Syncro Soft SRL

Effective Date: January 26, 2026

Document Version: 1.0

Next Scheduled Review: July 2026

1. Introduction and Regulatory Context

This document outlines the security posture and compliance alignment of Syncro Soft SRL in relation to the Digital Operational Resilience Act (EU) 2022/2554 ("DORA"). As a provider of Commercial Off-The-Shelf (COTS) software installed on-premise, we acknowledge our role in supporting Financial Entities subject to DORA in meeting their regulatory obligations.

Oxygen XML Editor Suite consists of standalone desktop applications that operates entirely within the customer's own IT infrastructure. The software is installed directly on customer-owned devices, processes data locally, and does not transmit customer data to Syncro Soft or maintain any remote access to customer systems. This operational model means that customers retain complete control over the software deployment, configuration, data management, and operational resilience measures and applies uniformly across all products in the suite, regardless of functional specialization (authoring, development, or XML/JSON processing).

We recognize that while our software does not fall within the direct oversight framework for critical ICT third-party providers under DORA Chapter V Section II, Financial Entities using our product must conduct appropriate due diligence on all technology vendors as part of their ICT risk management framework under DORA Article 28. This statement is designed to assist customers in their compliance assessments and to demonstrate our commitment to security, transparency, and operational resilience.

This statement applies to all standalone, on-premise products included in the Oxygen XML Editor Suite, namely Oxygen XML Editor, Oxygen XML Developer, Oxygen XML Author, and Oxygen XML JSON Editor. All products covered by this statement share the same architectural principles, deployment model, security assumptions, and operational characteristics as described in this document.

2. Shared Responsibility Model

Given the on-premise nature of Oxygen XML Editor Suite, operational resilience responsibilities are clearly divided between Syncro Soft and our Financial Entity customers:

- **Customer Responsibilities:** Financial institutions using Oxygen XML Editor Suite are responsible for infrastructure security, including hardware maintenance, network security, and physical access control. They maintain control over data backup and recovery processes, identity and access management within their local environment, and the configuration of the software according to their security policies. Customers are also responsible for conducting their own security assessments, operational resilience testing, and ensuring the software is implemented in accordance with their ICT risk management framework. Any ICT-related incidents must be reported by customers in accordance with DORA requirements.
- **Syncro Soft Responsibilities:** We are responsible for the security of our software development lifecycle, delivery of security patches and updates, vulnerability management in our codebase, and providing comprehensive technical documentation for secure configuration and deployment. We maintain robust technical support services to assist customers with product-related inquiries and provide timely notification of security-relevant issues that may affect customer installations.

This clear delineation ensures that each party can focus on their respective areas of control and expertise while working collaboratively to support overall operational resilience.

3. Software Development and Supply Chain Security

We implement comprehensive measures to ensure the integrity and security of Oxygen XML Editor Suite throughout its development lifecycle:

- **Secure Coding Practices:** Our development team follows industry best practices, including OWASP standards, to prevent common vulnerabilities such as SQL injection, cross-site scripting, buffer overflows, and other security weaknesses. Code reviews are conducted as part of our quality assurance process to identify potential security issues before release.
- **Vulnerability Scanning and Testing:** We conduct regular static application security testing (SAST) and dynamic application security testing (DAST) of our source code. This includes automated scanning for known vulnerability patterns and manual security assessments of critical components. Our testing regime covers both our proprietary code and third-party libraries integrated into the product.
- **Software Integrity Protection:** All software binaries and installation packages are scanned for malware before distribution. Our releases are digitally signed to ensure integrity and authenticity, allowing customers to verify that the software has not been tampered with during download or

installation. We maintain strict access controls over our build and release infrastructure to prevent unauthorized modifications.

- **Dependency Management:** We actively monitor third-party components and libraries used within Oxygen XML Editor Suite to identify and mitigate supply chain risks. When security vulnerabilities are discovered in dependencies, we assess the impact on our product and take appropriate remediation action, including updating to patched versions or implementing compensating controls. We maintain an inventory of third-party components to facilitate rapid response when new vulnerabilities are disclosed.

4. Vulnerability Management and Patching

In alignment with DORA requirements for timely remediation of vulnerabilities, we maintain a structured approach to vulnerability management:

- **Vulnerability Identification and Reporting:** We maintain a formal process for receiving and investigating security vulnerability reports from customers, security researchers, and internal testing. Security-related inquiries can be submitted to our dedicated security contact: security@oxygenxml.com. We treat all vulnerability reports with appropriate urgency and confidentiality.
- **Risk Assessment and Prioritization:** When vulnerabilities are identified, we assess their severity based on factors including exploitability, potential impact, and affected versions. Critical vulnerabilities that could compromise confidentiality, integrity, or availability of customer systems are prioritized for immediate remediation.
- **Patch Development and Delivery:** Critical security patches are developed and tested on an accelerated timeline. We commit to notifying customers of any significant vulnerability discovered in Oxygen XML Editor Suite and providing remediation instructions, workarounds, or software updates as appropriate. Patch notifications include clear descriptions of the security issues addressed, affected versions, and recommended actions.
- **Software Support Lifecycle:** We provide clear documentation regarding the support lifecycle for all Oxygen XML Editor Suite versions, including end-of-life (EoL) and end-of-support (EoS) dates. This information assists Financial Entities in their transition planning and ensures they can maintain supported software versions in accordance with their operational resilience requirements. Customers are encouraged to maintain current versions to benefit from the latest security enhancements.

5. Incident Support and Response

While Oxygen XML Editor Suite operates entirely within the customer's environment and Syncro Soft does not have access to customer production systems or data, we maintain robust support capabilities to assist customers during ICT-related incidents:

- **Technical Assistance:** In the event of an ICT-related incident involving our software, Syncro Soft provides expert technical support to assist the Financial Entity in investigating the issue, identifying potential software-related causes, and implementing corrective actions. Our technical support team has deep knowledge of the product architecture and can provide guidance on troubleshooting, configuration issues, and potential software-related causes of operational disruptions.
- **Communication Channels:** We maintain dedicated support channels including email (support@oxygenxml.com), a support portal, and phone support to ensure customers can reach us rapidly during critical incidents. Support requests are tracked, prioritized, and escalated according to severity, with critical issues receiving immediate attention.
- **Incident Collaboration:** When requested, we work collaboratively with customer technical teams to investigate incidents that may be related to our software. While we cannot access customer systems directly, we can provide detailed technical information about product behavior, configuration options, and known issues that may be relevant to incident resolution.
- **Internal Incident Response:** We maintain internal processes for identifying, assessing, and addressing security vulnerabilities or quality issues in Oxygen XML Editor Suite. When we become aware of issues that may affect customer operations, we proactively communicate with affected customers and provide guidance on mitigation measures.

6. Audit Rights and Transparency

We understand Financial Entities' need for "rights of access, inspection, and audit" under DORA Article 30 and are committed to providing appropriate transparency into our security practices:

- **Technical Documentation:** We provide comprehensive technical documentation for Oxygen XML Editor Suite, including installation guides and security recommendations. This documentation supports customers' internal risk assessments and helps them configure the software in accordance with their security policies. Documentation is regularly updated to reflect product changes and security best practices.
- **Security Questionnaires and Due Diligence:** We respond to customer security questionnaires and due diligence requests, providing information about our software development practices, security controls, vulnerability management processes, and organizational security policies. We recognize

that Financial Entities must conduct appropriate vendor risk assessments and are committed to supporting these activities.

- **Third-Party Assessments:** We undergo periodic independent security assessments and testing of our software. While the detailed results of these assessments are proprietary, we can provide summaries or attestations under appropriate non-disclosure agreements to support customer compliance requirements.
- **Process Documentation:** We maintain documented processes for secure software development, quality assurance, release management, vulnerability handling, and incident response. Information about these processes can be shared with customers to support their understanding of our security posture and operational practices.

7. Business Continuity and Exit Strategy

To ensure the long-term operational resilience of our customers and avoid vendor lock-in concerns, we have implemented the following measures:

- **Data Portability:** Oxygen XML Editor Suite is designed to work with standard, open file formats (primarily XML, but also supporting numerous other standard formats for XML-related workflows). Customers retain full control over the storage and management of their documents and configurations. . This software allows Financial Entities to migrate to alternative solutions if necessary without losing access to their information.
- **Product Longevity and Support:** Oxygen XML Editor Suite has been in continuous development and active use since 2001, demonstrating over two decades of sustained product evolution and market presence. We maintain a consistent release cadence with regular updates that include new features, performance improvements, and security enhancements. This long-standing track record provides Financial Entities with confidence in the product's stability and our commitment to ongoing development. We provide clear communication about support lifecycles for different versions, including planned end-of-support dates, which allows customers to plan their technology strategies and upgrade paths with appropriate lead time.
- **Source Code Escrow:** Given the nature of Oxygen XML Editor Suite as a COTS application in a competitive market where alternative XML editing solutions are readily available, we do not offer source code escrow arrangements. Financial Entities using our software are not locked into a single-vendor dependency for XML editing capabilities, as the market provides multiple viable alternatives should the need for transition arise. The availability of competitive alternatives, combined with our product's use of standard file formats that ensure data portability, provides

Financial Entities with natural exit options and mitigates vendor concentration risk without requiring source code access.

- **Transition Assistance:** Should a customer decide to transition away from Oxygen XML Editor Suite, we provide reasonable assistance to ensure smooth migration.

8. Continuous Improvement and Regulatory Alignment

We are committed to continuous improvement of our security practices and to staying informed about evolving regulatory requirements:

- **Regulatory Monitoring:** We monitor developments in DORA implementation, guidance from European Supervisory Authorities, and related cybersecurity regulations to ensure our practices remain aligned with regulatory expectations. As implementation guidance evolves, we will update our processes and documentation accordingly.
- **Customer Feedback:** We value feedback from our Financial Entity customers regarding their compliance needs and security concerns. Customer input helps us prioritize security enhancements and improve our support for their regulatory obligations.
- **Security Investments:** We maintain ongoing investment in security capabilities, including tools, training, and processes that enhance the security of our software development and delivery practices. Security is an integral part of our product quality commitment, not an afterthought.

9. Contact Information

For questions regarding this statement or Oxygen XML Editor's security and operational practices, please contact:

- **Technical Support:** support@oxygenxml.com
- **Security Inquiries:** security@oxygenxml.com
- **General Information:** info@oxygenxml.com
- **Sales and Business Development:** sales@oxygenxml.com

10. Legal Disclaimer

Important Note: This statement is provided for informational purposes to assist customers in their DORA compliance assessments and vendor due diligence processes. Each Financial Entity is responsible for determining its own regulatory obligations, conducting appropriate risk assessments, and making independent decisions regarding the use of Oxygen XML Editor Suite within their operational environment.

Nothing in this statement constitutes legal or regulatory advice, nor does it create any contractual obligations beyond those specified in applicable license agreements and support contracts. Customers

with specific DORA-related questions or compliance concerns should consult with their legal and compliance teams and, if necessary, their regulatory supervisors.

Syncro Soft SRL makes no warranties regarding the suitability of Oxygen XML Editor Suite for any particular regulatory purpose. Customers are responsible for evaluating whether the product meets their specific operational resilience and compliance requirements.

This document may be updated periodically to reflect changes in our practices, product capabilities, or regulatory guidance The current version of this statement is always available on our website.