Last Updated 27 January 2026

Introduction

Numonix LLC, a Delaware limited liability company, take the availability and the protection of our customers data very seriously.

Our products are trusted within many regulated industries to handle privileged internal communication and customer interaction recording. This statement outlines the specific governance, management and resilience monitoring that Numonix has designed into its IXCloud product set to allow our customers to meet their compliance objective.

Numonix has mapped our externally assessed and certified processes against the key requirements within Act (EU) 2022/2554 known as the Digital Operational Resilience Act ("**DORA**"), which came into effect on January 17 2025. This statement is intended to provide the required confirmation specifically to those Numonix customers within the European Finance sector, but generally to any Numonix customer that needs to confirm resilience under its own security and governance processes.

Certified 3rd Party Audits

ISO 27001 Numonix maintains a continually monitored Information Security Management System (ISMS) that is independently certified to comply with ISO 27002:2022

SOC 2 Type II Numonix requires that all critical business, resilience, security, privacy, availability, policy, and operational controls required to deliver and operate IXCloud, a Secure by Design SaaS product, are fully assessed at a SOC2 Type II assurance level.

Data Protection

All recordings made within IXCloud supported services are collected over customer encrypted links and immediately stored using dedicated customer specific encryption methods.
Such protection means that no Numonix staff, at any level can have access to privileged or private data stored by any Numonix customer.

Access Control

All access is controlled, monitored and assessed against information security and access policies that require:

1. **Segregation of access**
   All identities are assigned to accounts with specific and segregated roles, MFA is mandatory for all access. Use of, or attempted use of incorrect accounts is classed as a security incident.
2. **Segregation of environments**
   Numonix policy requires that all development, test, and production environments are logically separate and require unique accounts for access. No production access account is permitted to access any non-production environment, and no non-production account can have access to any production resource.
3. **Segregation of authentication realms**
   All customer recorded data is accessible only to customer managed accounts. No Numonix accounts can have access to any encrypted customer data or customer process action.

Secure Software Design

Numonix follows a documented Secure Software Development Lifecycle that requires all code to be actively scanned during development, before release and continuously whilst in production.
Code integrity is maintained through developer training, tracking all code against author, and mandatory live secure application security testing within the Numonix SSDLC.

Active Vulnerability Management

All systems are actively scanned for internet visible vulnerabilities, and for any configuration or coding vulnerability within authenticated and non-internet accessible contexts.
The Numonix vulnerability management process ensures that no critical, high or medium level vulnerability remains unaddressed whether at a coding stage or within any deployed production environment.

Monitoring and Incident Management

All production systems are actively monitored and scanned. Application and storage access, encryption key use and management, and user privilege and change events are evaluated on collection and appropriately handled. Cybersecurity/SOC level events are reported to and handled by appropriately trained personnel.

Business Continuity and Service Availability

Numonix IXCloud is 100% built and operated high availability SaaS product within Microsoft Azure, and as such at a regional or global infrastructure level can have no higher levels of availability than that enabled by Microsoft itself. In respect of the IXCloud system itself Numonix conducts regular Business Continuity exercises to confirm that components, parts, or complete systems can be restored or full replaced within time frames equivalent to that of the supporting infrastructure.
All customer data is stored in high availability encrypted storage objects that may be backed up by customers using provided secure APIs should customers so require.

Contact Us

If you have any questions about our DORA Compliance Principles please submit a request by either:

Calling us at +1 (855) 686-6649 (domestic) or +1 (561) 952-2600 (international);

Contacting our Security Officer by email at dataprotection@numonix.cloud; or

Writing to us at:

Numonix LLC
Attn: Steve Jump, Chief Information Security Officer
150 East Palmetto Park Road, Suite 800
Boca Raton Florida, 33432 USA

Please allow up to 30 days for us to reply.