

CODEX™

Cybersecurity by design



Your Ally in Advancing Quality

CYBERSECURITY

BY DESIGN

CODEX™ is the Data Management Software for BACT/ALERT® 3D that enhances and optimizes the sterility testing process with the assurance of the highest level of data integrity compliance, and helping you take the right decision with greater insights.

SURVEILLANCE

- Defense-in-depth principles have been applied for securing CODEX™ by implementing state of the art development methods for providing maximum reliability.
- CODEX™ is scanned for cybersecurity vulnerabilities using an external reference tool.
- A cybersecurity bulletin is issued internally.

EXPERTISE

- Either at rest or in transit, bioMérieux enforces data protection by implementing security features in compliance with current standards, such as cryptographic measures, role-based access control, or a strong backup and restore process.
- Using encrypted PostgreSQL database, confidentiality, integrity, availability and authenticity of all data processed by CODEX™ is ensured during its whole lifecycle.
- For every new CODEX™ software release, penetration tests are performed by external companies to detect new vulnerabilities.
- All vulnerabilities are assessed via risk assesment and corrected in a patch or next version if required.

PROACTIVITY

- Development and maintenance of CODEX™ are performed following a secure development lifecycle integrating mandatory security activities and in compliance with standards and guidelines such as 21CFR11.
- A cybersecurity risk assessment is performed prior to each CODEX™ release to ensure safety, security, and privacy.
- Continuous updates and upgrades are released for CODEX™, meaning that latest features and cybersecurity improvements are always made available for bioMérieux's customers.





How does CODEX™ address compliance following the highest international standards?

Benefits	Requirements	CODEX™ Features
Authentication & Authorization	Automatic logoff	CODEX™ forces automatic logoff after a customizable period of inactivity.
	Authorization	CODEX™ leverages Windows user rights management and build-in Software Accounts Authorization, which enables role-based access control. CODEX™ applications are designed to run in non-administrative operating system accounts to prevent tampering.
	Person Authentication	CODEX™ manages people authentication via integrated account management or via LDAP/LDAPS
	Configuration of Security Features	The software authentication service can be configured (based on three levels) according to the security policy of the customer.
	Node Authentication	CODEX™ implements authentication using JWT tokens.
Availability	Network Controls	CODEX™ is hosted in the customer's environment; therefore, the use of a firewall is recommended. Additionally, CODEX™ authorizes only the necessary ports for its operation.
	Digital Certificates	The customer can use their own certificates from a recognized authority.
	Malware Detection/Protection	The customer can install their corporate anti-malware solution, and apply their own security policy.
	Web Browser Compatibility	CODEX™ is compatible with Edge, Firefox, and Chrome.
Data	Classification(s) of Data Stored	CODEX™ doesn't store or processes any sensitive data, but it could eventually store personal data like usernames.
	Archiving	CODEX™ enables authorized users to generate data archives for a customizable period of time.
	Data Backup and Disaster Recovery	CODEX™ enables authorized users to automate backups in an encrypted format and store them on a local or network drive (prerequisites applicable). The system can be restored to a prior date with the assistance of bioMérieux support.
	Transmission Confidentiality	Data is encrypted using AES 256. TLS 1.2 and TLS 1.3 are supported.
	Transmission Integrity	Enabling TLS 1.2/1.3 for communications grants native transmission integrity by protocol design.
Audit	Audit Controls	Audit Trail records cannot be deleted, are stamped and can be exported.
	Regulatory Compliance	CODEX™ is designed to help customers meet 21 CFR Part 11 compliance.
	Electronic Signature	CODEX™ allows electronic signature for bottle and sample approval.
Maintenance	System and Application Hardening	Cybersecurity risk assessments, penetration testing, SAST (static application security testing), SCA (software composition analysis), and manual code review are performed and vulnerabilities are remediated (if required) as part of the secure SDLC (software development lifecycle) to ensure the application is hardened appropriately.
	Cybersecurity product updates	Periodic updates will be available, as needed to remediate discovered vulnerabilities.
	Third-party Components in Product Lifecycle Roadmaps	SBOM (Software Bill of Materials) is generated at each product release, to identify libraries and third-party components utilized to ensure all components and libraries stay up to date.
Other	Security Guides	A detailed Product Security Whitepaper will be available for CODEX™ (under NDA).
	Scope	This assesment is applicable for CODEX™ Version 1.X