BIOMÉRIEUX

MAESTRIA™
CYBERSECURITY

MAESTRIA™

PIONEERING DIAGNOSTICS

CYBER SECURITY

A SET OF PROACTIVE MEASURES (CYBERSECURE BY DESIGN), SURVEILLANCE AND CORRECTIVE MEASURES.

Cybersecurity is now integrated as soon as possible in the design of our products. Supported by our partners and experts in cybersecurity and data privacy, bioMérieux has implemented a Secure Development Lifecycle that ensures Security and Privacy by Design.

Learn more: https://www.biomerieux.com/corp/en/our-offer/cybersecurity.html
In case of specific questions, please e-mail PrivacyOfficer@biomerieux.com

SURVEILLANCE

EVERY WEEK

- MAESTRIA™ platform is scanned for cybersecurity threats using an external reference tool

EVERY MONTH

- All vulnerabilities are assessed (impact/criticality) and corrected in a patch if relevant
- A cybersecurity bulletin is issued internally

EVERY RELEASE

- For every new MAESTRIA™ release & platform, penetration tests are performed by external companies
- Each MAESTRIA™ release integrates cybersecurity updates

EXPERTISE

CYBERSECURITY RISK ANALYSIS

- As for product safety, a cybersecurity risk analysis is performed on each MAESTRIA™ release

- This cybersecurity risk analysis and cybersecurity state-of-the-art good practices are an input to MAESTRIA™ developments and architecture design

PROACTIVITY

SUPPORT BY SECURITY EXPERTS

- Our security partners bring skilled staff , experience and proven coding methodology in development of highly sensitive platforms (Department of Defense, Space industry)

- Recognized as key leaders in Cybersecurity

ISO 80001 REQUIREMENTS	MAESTRIA™ FEATURES
Automatic logoff	The system automatically logs off users based on a configurable period of inactivity.
Audit Controls	Audit Trail records cannot be deleted, are stamped and can be exported.
Authorization	MAESTRIA™ 5.0 leverages Windows user rights management which enables role-based access control. MAESTRIA™ 5.0 applications are designed to run in non-administrative operating system accounts to prevent tampering.
Configuration of security features	The MAESTRIA™ 5.0 system enables authorized users to configure user rights for various system functionalities such as modifying instrument configuration, audit trail and user management.
Cyber security product upgrades	bioMérieux maintains a monthly postmarket monitoring and patching of potential vulnerabiltes
Health Data De-identification	Health data are encrypted for backups and for support purposes. Data that are extracted for support purposes are de-identified.
Data Backup and Disaster Recovery	The MAESTRIA™ 5.0 system enables authorized users to automate backups and retention settings, as well as configure data backups in an encrypted format and stored on a local network or server.
Health Data Integrity & Authenticity	The system includes integrity monitoring features that alert on potential failures that could affect data integrity, including database referential integrity to prevent data corruption.
Malware Detection/Protection	Microsoft Windows Defender anti-virus software is installed by default on the system. The customer can also install the anti-virus of his choice and apply his own security policy.
Node Authentication	MAESTRIA™ 5.0 communicates with other elements of the Network in a secure way.
Person Authentication	The service providing authentication to the system can be configured according to the customer's security policy and associated with a Windows centralized authentication provider. The web login interface of the MAESTRIA™ 5.0 system can be integrated on the customer authentication service.
Third-party Components in Product Lifecycle Roadmaps	bioMérieux monitors components for emerging vulnerabilities and issues product update.
System and Application Hardening	bioMérieux conducts independent third party testing of the device operating system and network settings, including active ports and services.
Security Guides	bioMérieux publishes technical and architectural guidance for the secure deployment and configuration of devices, including security whitepaper, MDS2, and SBoM.
Health Data Storage Confidentiality	The system enables encryption of backups.
Transmission Confidentiality	The system supports HTTPS with TLS 1.2 encryption.
Transmission Integrity	The system is able to detect and recover from communication failures for critical messaging.
Other	The system runs Windows® 10 IoT (LTSB 2016), Windows® 10 IoT (LTSC 2019), Windows® Server 2016 or Windows® Server 2019.

GDPR

HIPAA COMPLIANT

bioMérieux Privacy Statement

The protection of personal data and respect of privacy are fundamental rights derived from the Universal Declaration of Human rights of 1948. bioMérieux is committed to protecting the confidentiality of the personal data of its employees and stakeholders.

Many countries have tightened regulations restricting the use and disclosure of personal data (e.g.US HIPAA Federal law, EU GDPR). These laws require companies to take steps to ensure the confidentiality, integrity and availability of this kind of data. bioMérieux deployed a compliance program regarding regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 which has entered into force in May 25, 2018 (GDPR) as well as national French laws.

bioMérieux has officially designated a Data Protection Officer (DPO) to the French Data Protection Authority (CNIL) to control and ensure compliance of the Company with this regulation.

bioMérieux S.A.
69280 Marcy l'Etoile • France
Tel.: + 33 (0)4 78 87 20 00 • Fax: +33 (0)4 78 87 20 90
www.biomerieux.com