PRODUCT CYBERSECURITY POSITION PAPER

Cybersecurity

Background

Bio-Rad management is aware of customer concerns related to Cybersecurity regulations while using connected medical devices. We at Bio-Rad are committed to supporting these customer needs.

We have established a Product Cybersecurity Center of Excellence (PC-CoE) to manage and lead all aspects of Bio-Rad's product Cybersecurity program that include development and deployment of:

- Cybersecurity by design
- Cybersecurity risk management
- Patch Management
- Incident Management
- Third party software solutions

Bio-Rad management is committed to developing instruments and software solutions that help facilitate best practices around Cybersecurity.

Cybersecurity by Design

We have added Cybersecurity related activities to our software development lifecycle (SDLC). Bio-Rad's Cybersecurity measures are integrated into each stage of Bio-Rad's SDLC to assure that Cybersecurity requirements are met by design.

We also realize that in addition to processes and technology, employee awareness is key to achieving a culture that is sensitive to Cybersecurity issues. To this end, we have implemented Cybersecurity training for our R&D and customer facing employees.

Cybersecurity risk management

Cybersecurity risk management involves identifying instrument risks and vulnerabilities and applying administrative actions and comprehensive solutions (home-grown or third-party) to make sure the instrument is adequately protected.

Bio-Rad adopted practices, that align to NIST framework (consists of standards, guidelines, and best practices) to manage Cybersecurity-related risks. These practices help promote the protection and resilience of the instrument.

Patch Management

In the Diagnostics industry, computer-controlled instruments and software products are potentially susceptible to Cybersecurity threats. This is true for Bio-Rad also. We will continue to address these issues with timely Cybersecurity updates ("patches"). Many of these updates are urgent. The objective of the Patch Management procedure is to define the process for:

- Evaluating Cybersecurity updates that may apply to Bio-Rad products
- Installing Cybersecurity updates to protect Bio-Rad products at customer sites

The process supports both, regular and urgent (per incident) Cybersecurity threats.

BIO-RAD

Third party software solutions

To protect Bio-Rad's equipment and to ensure its continued integrity and safe result delivery Bio-Rad does not permit any unauthorized third party software installation by the customer (e.g., anti-virus, system patches, firewalls, etc.). Unauthorized modifications to Bio-Rad instrument could change the regulatory status of the device and cancel customer's warranty. Any abnormal behavior of Bio-Rad solution which is a result of such modification is not covered under Bio-Rad's service agreements. Such modifications can affect the performance or safety of the device in unpredictable ways. Therefore Bio-Rad is not responsible for instrument that has been subject to such modification.

Bio-Rad is continuously evaluating and examining its products to ensure that they continuously accommodate Cybersecurity needs as the market and risks keep changing and evolving. This is an on-going effort and we are open to discuss Cybersecurity issues with clients – our true partners – in order to meet their evolving needs and for facing the Cybersecurity frontier together.

Incident Management

Bio-Rad's BRiCare solution continuously monitors software and hardware behavior of Bio-Rad's instruments used by customers. The received information and alerts help identify Cybersecurity threats and incidents. BRiCare, in addition to monitoring, can also provide remote support and immediate remediation when such need arises.

BIO-RAD

Bio-Rad Laboratories

Clinical Diagnostics Group

Website *www.bio-rad.com/diagnostics* ***Australia*** *+61(2)9914-2800* ***Austria*** *+43-1-877-8901* ***Belgium*** *+32(3)710-53-00* ***Brazil*** *+55(31)3689-6600* ***Canada*** *+1 514 334-4372* ***China*** *+86-21-61698500* ***Czech Republic*** *+420-241-430-532* ***Denmark*** *+45-4452-1000* ***Finland*** *+358-9-804-22-00* ***France*** *+33 1 47 95 60 00* ***Germany*** *+49(0)89-318-840* ***Greece*** *+30-210-7774396* ***Hong Kong*** *+852-2789-3300* ***Hungary*** *+36-1-459-6100* ***India*** *+1-800-180-1224* ***Israel*** *+972-3-9636050* ***Italy*** *+39-02-216091* ***Japan*** *+81-3-6361-7070* ***Korea*** *+82-2-3473-4460* ***Mexico*** *+52(55)5488-7670* ***The Netherlands*** *+31-318-540666* ***New Zealand*** *+64-9-415-2280* ***Norway*** *+47-23-38-41-30* ***Poland*** *+48-22-3319999* ***Portugal*** *+351-21-472-7700* ***Russia*** *+7-495-721-14-04* ***Singapore*** *+65-6415-3170* ***South Africa*** *+27-11-442-85-08* ***Spain*** *+34-91-590-5200* ***Sweden*** *+46-8-555-127-00* ***Switzerland*** *+41 26 674 55 05/06* ***Taiwan*** *+886-2-2578-7189* ***Thailand*** *+662-651-8311* ***United Kingdom*** *+44(0)20-8328-2000*