Accuray Product Cybersecurity Policy Statement

- Accuray recognizes that trust is essential for organizations and customers to fully embrace and benefit from our technologies. We are committed to providing customers with secure radiation treatment products they expect, and to have confidence in Accuray as their preferred radiation therapy product provider. Our cybersecurity policies and practices are continuously evolving to harmonize with leading industry standards, complementing more than two decades of experience in delivering innovative, life saving, and reliable products.
- Cybersecurity is a critical element in Accuray's approach to securing its computing environment. In an ever-changing threat environment, our development teams strive to employ rigorous cybersecurity practices, which are imbedded into Accuray's Secure Development Lifecycle (SDL). The SDL process is now integrated with the product development lifecycle from requirements to design to implementation. Various phases of the SDL process emphasize secure software development practices, and dictate specific activities and processes be applied as appropriate to each phase of product development.

Accuray Product Cybersecurity Policy Statement

Accuray's Cybersecurity Objectives Strive To :

- Security by Design
  - Develop products using a Security by Design philosophy throughout each phase of product development in accordance with the Accuray security development lifecycle process to help ensure confidentiality, integrity, and availability.
- State of the Art Security
  - Update security controls, features and procedures in harmony with new security technologies that reasonably protect Accuray products from current and future threats to confidentiality, integrity, and availability.
- Defense in Depth
  - Design Accuray products with multiple layered security controls through access control, application security, network security, system security and detection, to reduce attack surface, minimize incident impact, and respond to events.
- Risk-based Approach to Cybersecurity
  - Consistent with industry practices, rely on a risk-based cybersecurity approach to identify, prioritize and allocate resources to achieve measurable cybersecurity risk reduction.
- Cyber Resilience
  - Continuously enhance organization's cyber resilience to address rapidly changing cyber landscape with agility.
- Lifecycle Management
  - Monitor post-market vulnerabilities and provide security patches and updates in a timely manner.
- Compliance
  - Harmonize industry best practices and standards, and maintain compliance with global laws and regulations.