

Product Security Statement

This paper summarizes the Ertunc Ozcan position on securing our products, services, applications, and systems and describes our processes for providing products with Security Designed In.

Background

We at Ertunc Ozcan recognize that the security of Ertunc Ozcan NICU products and services are an important part of our security planning. We are dedicated to helping you maintain the confidentiality, integrity, and availability of personal data, business data, and the Ertunc Ozcan hardware and software products that create and manage this data.

Threats to the security of devices and personal and healthcare information continue to increase. These threats include malicious security attacks via viruses, worms, and hacker intrusions.

To fulfill our commitment to security, we at Ertunc Ozcan maintain a cyber security program to: develop, deploy, and support advanced security features for our products and services.

Manage security events in the field. Ertunc Ozcan participates in industry and government collaborations to help ensure product innovations and clinical information is produced and available at the highest level of quality, availability, and confidentiality.

We implement security within a heavily regulated medical device industry. Government regulations (e.g., those of the US Food and Drug Administration (FDA), European Commission) require that hardware and software changes be subjected to rigorous verification and validation to ensure high safety and performance standards are met in all Ertunc Ozcan medical devices.

Likewise, Ertunc Ozcan strives to ensure that same high standard for NICU products and services. Organization Ertunc Ozcan operates under a Product Security Policy governing Security Designed In creation of products and services.

The policy also governs risk assessment, identification of vulnerabilities in existing products, and incident response activities.

