Rambus

Information Security Policy

At Rambus, we are conscious that Information Security is an essential part of our business, customers and stakeholders. We are fully committed to the Information Security Policy. All personnel including third parties (contractors, subcontractors or consultants) accept their roles and responsibilities in implementing, maintaining and conforming to the Rambus Information Security Policy. Violations of this policy may result in all related personnel being subject to disciplinary action up to and including termination.

Information security plays a pivotal role in a companywide continuous improvement program. By adopting best practice methodology, we strive to deliver high security robust products and services that meet our customer expectations, with the aim of retaining our existing customers and increase the overall customer base.

The Information Security Management System includes security policies, procedures and guidelines developed in accordance to the ISO27001 Standard and is designed to abide by laws, regulations, and agreements with suppliers, contractors and clients. To achieve the aforementioned goals:

- The company promotes information security awareness and provides appropriate information security training for all staff and associates;
- The company monitors for, investigates, and acts upon all breaches of information security, actual, or suspected;
- Maintain and verify the established and implemented information security controls at regular intervals;
- Safeguard the confidentiality, integrity, and availability of information assets and processing methods; and
- Store all electronic information in leading industry standard formats to ensure future proofing.

Luc Seraphin
Chief Executive Officer
June 29, 2018

Mark Grimse
VP, Information Technology