
Information Security Policy

Founded in 2016, RapidDeploy provides telecommunicators, first responders and 911 agencies with Next Generation technology solutions that deliver intelligent information and drive better outcomes in mission critical situations. We are innovators that are changing traditional 911 paradigms, transforming emergency response and improving the efficacy of 911.

Our cloud-native, integrated platform processes big data at scale, unifies communications and visualizes information in a connected ecosystem— streamlining emergency response, driving life-saving outcomes and improving the efficacy of 911.

Our mission is to save lives by reducing response times.

RapidDeploy is fully committed to ensuring the Confidentiality, Integrity and Availability of the data entrusted to us.

RapidDeploy recognizes the disciplines of confidentiality, integrity and availability in Information Security Management are integral parts of its management function. The management of RapidDeploy views these as primary responsibilities and fundamental to the best business practice of adopting appropriate Information Security Controls.

RapidDeploy's Information Security policy seeks to operate to the highest standards continuously and to focus on continual improvement through annual review.

We will:

- Comply with all the applicable laws, regulations, and contractual obligations.
- Implement continual improvement initiatives, including risk assessment and risk treatment strategies, while making the best use of its management resources to better Information Security requirements.
- Communicate our Information Security objectives, and its performance in achieving these objectives, throughout the organization and to interested parties.
- Adopt an Information Security Management System comprising organizational policies and procedures which provide direction and guidance on information security matters relating to employees, customers, suppliers and interested parties who meet its work.
- Work closely with our customers, business partners and suppliers in seeking to establish appropriate Information Security standards.
- Adopt a forward-looking view on future business decisions, including the continual review of risk evaluation criteria, which may have an impact on Information Security.
- Train all members of staff in the needs and responsibilities of Information Security Management.
- Constantly strive to meet, and where possible exceed, our customer's, staff, and partners expectations.

Responsibility for upholding this policy is truly organization-wide under the guidance and with the assistance of the CISO(VP Engineering) who encourages the personal commitment of all staff to address Information Security as part of their skills.

Each business unit within RapidDeploy is required to apply this policy to ensure that they conform to RapidDeploy's information security standards with assistance from RapidDeploy Engineering.

Any questions regarding this policy can be directed to security@rapiddeploy.com