RTC Manufacturing understands that trust and security are of utmost importance to the agencies that we work with, which is why we have made these issues a priority in our business. Outlined below is a summary of our security practices and protocols. If you’d like additional information, please call us at 800.782.8721.

GENERAL
Due to strict security practices/protocols and the controlled impact of a breach, there have been no successful security breaches of any kind involving RTC Manufacturing, Inc. systems since the company’s inception in 1987.

FIELD EQUIPMENT
Traffic Cabinet doors should remain shut and locked if not in use. RTC Guardian Door Switches provide additional security to notify a user via text or e-mail each time a cabinet door is opened. If a cabinet is breached and a Time Switch is used to change schedule programming, the changes are made only to the one breached location. The changes will only exist locally until the time switch checks in with the database and the programming gets overwritten each morning. Without proprietary information, no other RTC Field Equipment can be used to access/change the database or server.

DATA NETWORK
RTC utilizes a third party data network with tier one data carriers. The data carriers own and secure the hardware infrastructure. To access any raw transmissions, a successful breach would require access to both the carrier and the network provider.

SERVERS AND DATABASE
RTC uses multiple, unique password-protected servers located off-site. Access to the SQL database is tightly controlled through XML transmissions that exclusively use HTTPS protocols. There is absolutely no direct access to the RTC database.

SOFTWARE
All versions of the RTC Connect software suite (mobile, web-hosted, and client-hosted) are password protected. Specific user log-in credentials and permissions exist for intra-office protection. The client-hosted application does not require an Internet connection to RTC servers, except for M2M installations.

ADDITIONAL MEASURES
The access point most susceptible to breach is a computer running the client-based version of RTC Connect or the mobile/web-hosted version with an auto-saved password. We strongly suggest using unique passwords for your computer and software log-ins. We also recommend logging out from the software completely at the end of use. For your protection, RTC does not allow for agency passwords to be changed from within the software.