Setra CEMS™ Software
Product Security Statement

Document #	SS-CEMS-ProductSecurityStatement-Rev B
Created By	Samantha S
Reviewed By	Patrick M

Setra Systems, Inc
159 Swanson Road, Boxborough, MA 01719
800.257.3872 • www.setra.com

1 Purpose

Setra CEMS™ Software is our Software as a Service (SaaS) platform for environmental monitoring of critical spaces and clean room environments. The purpose of this document is to detail how Setra Systems security and privacy practices have been applied to CEMS, what you need to know about maintaining product security, and how we can partner with you to ensure security throughout this product's life cycle.

2 Security Principles

At Setra Systems, security is embedded in all aspects of our innovations, products, systems and services. We recognize that an effective product security process needs to be in place for the entire product life- cycle, including the design, development, production, deployment, maintenance and disposal of a product and any associated data. Setra's security approach is founded on the below principles:

2.1 Security is one of our priorities

Built with security in mind, our products are secure by design. We apply a risk-based approach that recognizes the intended use, user environment and other important factors to determine the level and type of security required.

2.2 Governance and Administrative Controls

Setra Systems does not and will not ever share customer data with third parties. Administrative access to customer data is heavily restricted and closely managed. Access to production systems and data follows the security standard of least privilege.

2.3 Partner Controls

Setra Systems holds its partners and vendors to the same standards to which we hold ourselves.

2.4 Open Communications and Responsible Disclosure

Setra Systems will inform customers and other impacted stakeholders of vulnerabilities and incidents that could impact the safety and security of our products.
It is important to realize that our security program is a growing and maturing practice. We operate under continuous improvement to push the bar on security features and robustness in our products.

3 Software and Security

CEMS is built on top of Amazon Web Services (AWS), which is compliant with a wide variety of industry- accepted security standards. Additionally, our engineers utilize proven and state-of-the-art security technologies and techniques, apply security guidelines derived from many organizations such as Open Web Application Security Project (OWASP), including specific countermeasures for OWASP Top Ten Vulnerabilities, in order to protect all systems, data, and information from unauthorized access in the best possible way. Vulnerabilities, in order to protect all systems, data, and information from unauthorized access in the best possible way.

3.1 Data Storage and Collection

All data collected and stored by CEMS, including backups are encrypted by industry standard AES-256 algorithm. The below list contains notable data collected by CEMS:

- Environmental data - e.g., pressure, temperature, humidity, etc.
- Name, email id, mobile phone number (if entered) of users.
- Asset information - building address, floor/room names, floor plans, device serial numbers, and device locations.

3.2 Data Backup and Availability

Data redundancy and high availability is built in to CEMS by ensuring that the database maintains 6 copies of data across 3 geographically separated locations to ensure automatic recovery in an unlikely event of primary database failure. In addition to automated recovery, scheduled automated backups are in place to trigger daily backups.

3.3 Data Communication

All traffic to and from our CEMS software platform is encrypted using the SSL/TLS V1.2 protocol with strong TLS cipher suites. User access to CEMS web portal is limited to HTTPS only. Firewalls have been put in place and default to deny all policy combined with required exceptions to open required ports only (80/443 and 8883).

3.4 Access Control

Access to CEMS portal is only through valid and unique credentials. CEMS enforces a strong password policy with minimum password strength requirements and regularly scheduled expiring passwords. Unauthorized attempts to login are blocked and logged.

3.5 Report vulnerability

Setra Systems values responsible reporting and disclosure of any vulnerabilities found in our platform. Please write the details of suspected vulnerability with Setra by sending an email to SetraCEMS@setra.com

3.6 Your Responsibilities for Security

Setra recognizes that the security of our products and services is an important part of our customers security and IT strategy. In practice, however, security is a responsibility shared by product manufacturers, providers of products and services, customers, and end-users. In order to use the CEMS security features effectively, we suggest you appoint at least one administrator. Administrator duties include but are not limited to:

- Creating/disabling users and roles.
- Reviewing audit logs and activity in the software for irregularities
- Setting up a password loss management procedure

Additionally, users should secure the SetraEDGE and other networked devices from unauthorized physical access.