Interact City

security measures

Protecting your data at all times
Keeping your data safe and secure

**Ensuring confidentiality**
Interact City provides a wide range of functionality covering all daily operations, for which dedicated user roles are assigned. Users are assigned different levels of access depending on authorization. Each user sees only the data specifically required for their needs and can execute only authorized operations (least privilege principle). In addition, data from individual customers is kept strictly separate and cannot be accessed by unauthorized users.

**Strong passwords and two-factor authentication**
Interact City requires a strong password for login. Two-factor authentication—known from banking applications—prevents logging into Interact City from an unauthorized computer.

When two-factor authentication is activated, access to an Interact City account will require the user’s password plus a verification code that is sent to the user’s phone or email. If the user fails to enter the code within 30 seconds, the login attempt will fail.

**Dedicated user roles**
Interact City offers SaaS (software as a service). We store data in multiple locations, arrange continuous synchronization, and use professional centers that provide the highest level of security and availability. The service runs on virtual servers with data continuously backed up in a separate data center with automatic rollover for high availability.

**Fully encrypted**
Data integrity ensures that all streetlight schedules are executed as specified. All streetlight switching points are logged to the Interact City system and are visible only to authorized users. Interact City is the central point of a wide communication network. All network communication is encrypted from the end points to the central servers.

**Tamper-proof**
Only authorized and registered devices can communicate with Interact City. Devices are registered with a unique secure key during the factory process and only these devices can communicate with Interact City. Devices are registered with a unique secure key during the factory process and only these devices can connect to the system. This prevents unauthorized third parties from tapping the communication and tampering with data during transmission. Traffic to and from registered devices is monitored closely to automatically detect any possible attacks, such as denial of service (DoS), misuse, or theft. All data is regularly backed up and encrypted while stored.

**Input validation**
Input is validated based on pre-defined data types (numbers, string fields) to avoid the entry of incorrect data formats. In addition, Interact City provides data property catalogs which can be defined and pre-set by the user.

**Reliable communication**
Interact City uses cellular IP and radio frequency networks for communication between field devices and servers. These networks are professionally maintained and provide the most reliable machine-to-machine communications service. For example, cellular networks use end-to-end encryption, and communication between the luminaire and server uses COAP, DTLS and UDP protocols. Communication between servers and light points is designed and encrypted to provide a high level of security. It results in proper authentication and data integrity while making efficient use of all data traffic. Interact City filters all the data to prevent fraud and tampering, and enforces strict firewall rules between the communication device and the central server. Filters include support, protocol, source IP and destination IP. The outdoor luminaire controller (the node) will only accept data from the Interact City server, not from other nodes or outside sources.

**Guaranteeing service**
Interact City offers SaaS (software as a service). We store data in multiple locations, arrange continuous synchronization, and use professional centers that provide the highest level of security and availability. The service runs on virtual servers with data continuously backed up in a separate data center with automatic rollover for high availability. Our infrastructure supplier and data center is certified to SOC1, SOC2 and ISO 27001, and is regularly audited. All backed-up data storage is encrypted.

**Securing operations**
Interact City delivers overall system security through a set of cybersecurity strategies that include strict operational processes. Such processes for account management, for example, enforce administrative policies. These processes also ensure that the latest web server updates are in use, and that the test and production environments are separated. Monitoring the traffic and identifying the threat situations are also key processes.

**Avoidance of downtime**
Interact City maintains the technical infrastructure while following the latest industry standards, avoiding downtime and maximizing availability of services.

In the unlikely event of a partial or total failure of the central Interact City infrastructure, redundant systems in different locations will take over automatically and the data will be saved securely in different locations. Maintenance announcements inform users about planned maintenance work and specific timing for when the service will be temporarily down. We always aim to minimize the impact on business hours of users.

**Highly robust**
The technical design of Interact City ensures that the failure or temporary non-availability of a device connected to Interact City does not block or degrade the service. Data is always kept consistent and issues are displayed to users. If a communication device is malfunctioning and creating malicious traffic, it will be blocked to save the integrity of the overall system. Additionally, the separation of each customer’s data prevents any potential technical problem from impacting other customers.

**Fall-safe operation**
In the unlikely event of a total failure of the Interact City infrastructure, the streetlights will continue to function according to pre-loaded schedules. Operational data such as energy data and faults are stored for days until the system is up and running again. With this feature, lighting in the street is not affected by the non-availability of Interact City. The system will auto-synchronize as soon as it is available again.

**Constant reviews**
Interact City regularly reviews its security procedures—including support from external experts—and continuously monitors security alerts. These measures ensure that organizational, technical infrastructure and security procedures are all kept up to date.

Optimizing availability

**Regular updates**
Maturing software development and release procedures guarantee consistent high quality of the Interact City software. Frequent and regular software releases ensure a rapid response to incidents. All releases are thoroughly tested to prevent accidental data modification and to provide data consistency. This also includes security-related test cases. The system conducts regular penetration tests and involves independent third parties to maintain high level security standards.

**Avoidance of downtime**
Interact City maintains the technical infrastructure while following the latest industry standards, avoiding downtime and maximizing availability of services.

In the unlikely event of a partial or total failure of the central Interact City infrastructure, redundant systems in different locations will take over automatically and the data will be saved securely in different locations. Maintenance announcements inform users about planned maintenance work and specific timing for when the service will be temporarily down. We always aim to minimize the impact on business hours of users.

**Highly robust**
The technical design of Interact City ensures that the failure or temporary non-availability of a device connected to Interact City does not block or degrade the service. Data is always kept consistent and issues are displayed to users. If a communication device is malfunctioning and creating malicious traffic, it will be blocked to save the integrity of the overall system. Additionally, the separation of each customer’s data prevents any potential technical problem from impacting other customers.

**Fall-safe operation**
In the unlikely event of a total failure of the Interact City infrastructure, the streetlights will continue to function according to pre-loaded schedules. Operational data such as energy data and faults are stored for days until the system is up and running again. With this feature, lighting in the street is not affected by the non-availability of Interact City. The system will auto-synchronize as soon as it is available again.

**Constant reviews**
Interact City regularly reviews its security procedures—including support from external experts—and continuously monitors security alerts. These measures ensure that organizational, technical infrastructure and security procedures are all kept up to date.