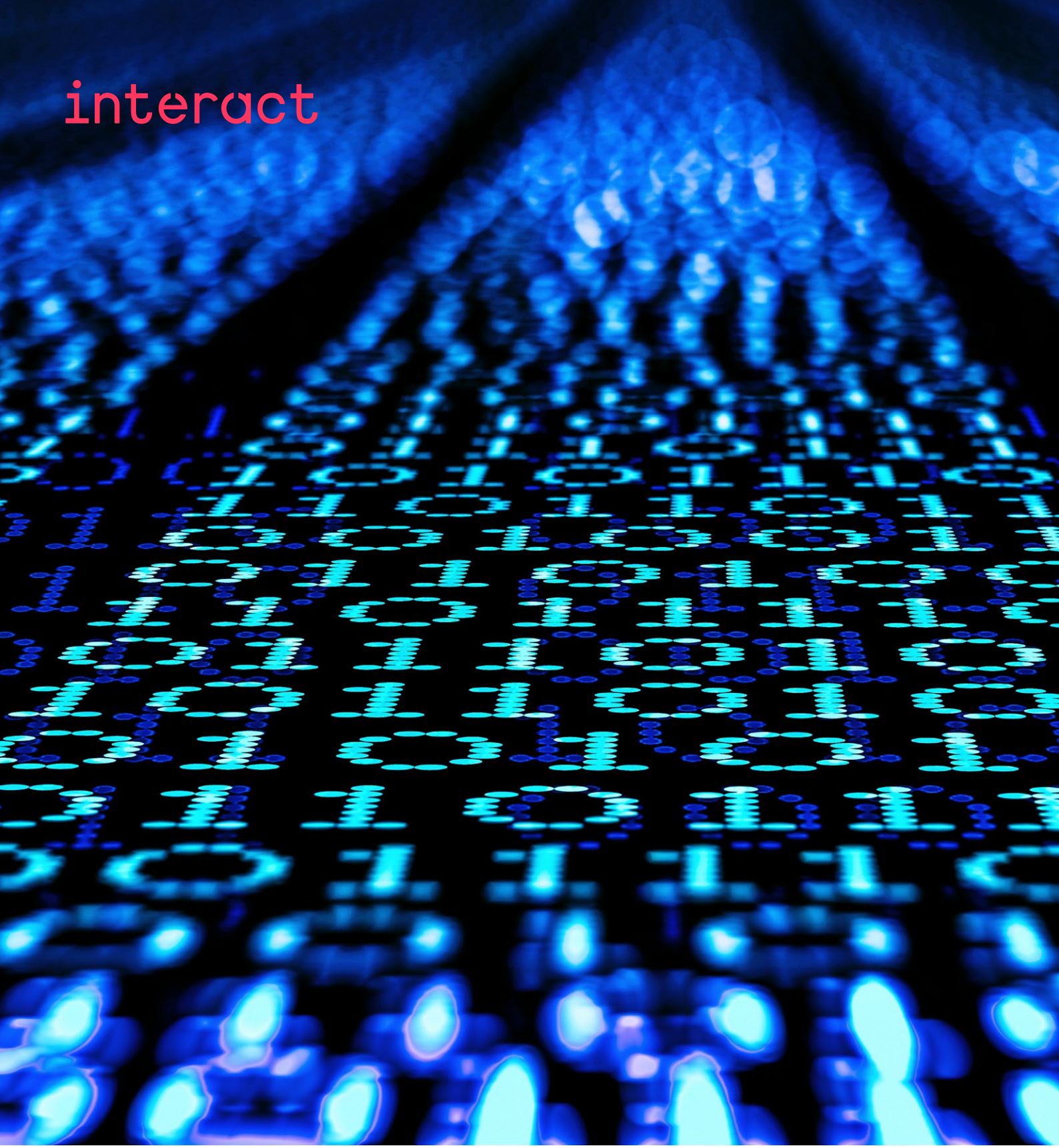
interact



Interact security measures

Protecting your smart street lighting data at all times

Keeping your data safe and secure

IT security is central to Interact, and the system is designed to maintain the confidentiality, integrity, and availability of your data. Interact used for smart street lighting meets the latest IT security standards and delivers on the promise of complete system security by establishing a set of cybersecurity strategies for data governance and privacy. These strategies apply to account management, updating web servers, monitoring data traffic, and identifying threat situations. They protect the system while accounting for dedicated failover and disaster recovery contingencies.

Our policies and processes are in accordance with the global standards, such as ISO/IEC 27001—Information Security Management Systems (ISMS), and we are the first lighting company to be certified to IEC 62443-4-1. IEC 62443-4-1 is a security certification for product development processes which ensures that all identified security requirements are implemented, verified, tested, and documented with traceability. It includes security risk analysis and threat modeling, code analysis verification and validation testing, and continuous vulnerability management assessment. Our business processes are internally and externally audited on a regular basis.

Ensuring confidentiality

Dedicated user roles

Interact 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 (Principle of Least Privilege). In addition, data from individual customers is kept strictly separate and cannot be accessed by unauthorized users.

Strong passwords and two-factor authentication

Interact requires a strong password for login. Two-factor authentication—known from banking applications—prevents any unauthorized computers from logging into the system.

When two-factor authentication is activated, access to an Interact account will require the user's password plus a verification code that the user will be sent. The user is informed about all unsuccessful login attempts and the last successful login.

After several unsuccessful login attempts, the user account will be blocked for one minute to protect the system against brute force attacks. The user will also be notified of any further unsuccessful login attempts that take place after they have logged in. Users can notify Interact support if they find anything suspicious. If potential threats to the system are detected, such as long spells of user inactivity or session hijackings, then the user will be logged out automatically.

Maintaining integrity

Fully encrypted

Data integrity ensures that all streetlight schedules are executed as specified. All streetlight switching points are connected to the system and are visible only to authorized users. Interact 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 the system. 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, the system provides data property catalogs which can be defined and pre-set by the user.

Reliable communication

Interact 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 the server, which 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 filters all the data to prevent fraud and tampering, and enforces strict firewall rules between the communication device and the central server. Filters include port, protocol, source IP and destination IP. The outdoor luminaire controller (the node) will only accept data from the server, not from other nodes or outside sources.

Regular updates

Mature software development and release procedures guarantee the consistent high quality of Interact 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.

Guaranteeing service

Interact 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 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.

Dedicated failover and disaster recovery plans exist for all these operational processes, ensuring that in the unlikely event of an outage the complete system can be restored.

Optimizing availability

Avoidance of downtime

Interact 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 infrastructure, 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 the system ensures that the failure or temporary non-availability of a device connected to Interact 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.

Fail-safe operation

In the unlikely event of a total failure of the Interact 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 Interact's non-availability. The system will auto-synchronize as soon as it is available again.

Constant reviews

Interact 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.

Security & privacy

For more information on security and privacy, please refer to our website:
www.signify.com/security

Find out what Interact can do for you

www.Interact-lighting.com/city

interact

© 2021 Signify Holding. All rights reserved. The information provided herein is subject to change, without notice. Signify does not give any representation or warranty as to the accuracy or completeness of the information included herein and shall not be liable for any action in reliance thereon. The information presented in this document is not intended as any commercial offer and does not form part of any quotation or contract, unless otherwise agreed by Signify. Philips and the Philips Shield Emblem are registered trademarks of Koninklijke Philips N.V. All other trademarks are owned by Signify Holding or their respective owners.