WHITE PAPER

Privacy and Data Security

OCCULIGHTS

01.09.2024

Security
Protocols in Occulights

Encryption for Communication:

Occu-Now AES-128 Encryption

Description: Secure device-to-device communication.

Benefit: Protects data from eavesdropping and tampering.

Wi-Fi Security with WPA2-PSK

Description: Uses WPA2-PSK to encrypt data transmitted over the local network.

Benefit: Prevents unauthorized access to data during transmission.

Internet Security Protocol:

WPA2-PSK

Description: A widely regarded secure encryption method for Wi-Fi networks.

Benefit: Ensures a secure connection to the local network and prevents unauthorized access.

Local Network Visibility:

Disabled Access Points

Description: Devices disable their own network broadcasting after connecting to Wi-Fi.

Benefit: Eliminates the possibility of attackers using these devices to infiltrate the main network.

Secure Boot and Firmware Updates:

Secure Boot

Description: Ensures only authenticated firmware can run on the devices.

Benefit: Prevents malicious software from being installed.

Over-the-Air (OTA) Updates:

Description: Allows for remote security patches and firmware improvements.

Benefit: Ensures devices stay secure without the need for physical access.

Access Control:

MAC Address Filtering:

Description: Restricts which devices can communicate with Occulight and Occu-Hub.

Benefit: Adds an extra layer of security by controlling device access.

Firewalls and Protection:

Software-Based Firewalls:

Description: Provide additional protection against unauthorized access and attacks.

Benefit: Strengthens device security by blocking potentially harmful connections.

Data Privacy and **Processing**

Data Anonymization

Anonymization of MQTT Messages

Details: Data sent from the HUB to AWS is anonymized to protect individual identities.
Example: The MQTT message structure and the specific fields involved, such as timestamps, temperature, humidity, and MAC addresses.
Privacy Assurance: Personal Identifiable Information (PII) is minimized, and fields that could contain PII (like MAC and IP addresses) are handled in a way that ensures they do not link to individual users.

Data Privacy Assurance

Data Encryption

Details: All communications are encrypted using TLS 1.2 or higher to prevent unauthorized access.
Benefit: Protects data during transmission, ensuring it cannot be intercepted or altered.
Access Controls:
Details: Role-based access controls (RBAC) and multi-factor authentication (MFA) restrict access to data.
Benefit: Ensures that only authorized personnel can access sensitive information.
Data Minimization:
Details: Only essential data is collected and transmitted, adhering to the principle of data minimization.
Benefit: Reduces the risk of privacy breaches by limiting the amount of data handled.
Anonymization Techniques:
Details: Pseudonymization or anonymization is applied where possible to protect user identity.
Benefit: Prevents the direct identification of individuals from the data.

Data Usage Policy:

Non-Commercial Use

Details: Data is used strictly for monitoring and control purposes and is not sold or shared for commercial purposes.

Benefit: Protects user data from being exploited for marketing or other commercial activities.

Data Retention:

Details: Data is retained only as long as necessary to fulfill its purpose, with anonymized data possibly retained for historical analysis.

Benefit: Ensures data is not kept longer than needed, reducing the risk of misuse.

Third-Party Agreements:

Details: Third-party providers involved in data processing are bound by strict data protection agreements.

Benefit: Ensures that data privacy standards are maintained across all external partnerships.

Incident Response and Data Breach Protocol:

Immediate Containment

Details: Protocols are in place to contain any data breach or security incident.

Benefit: Minimizes the impact of a breach by quickly stopping unauthorized access.

Assessment and Notification:

Details: Incidents are assessed, and affected parties are notified as per legal requirements.

Benefit: Ensures transparency and compliance with legal obligations.

Root Cause Analysis:

Details: Investigates the cause of the breach and implements corrective actions.

Benefit: Prevents recurrence by addressing the underlying issue.

Reporting and Documentation:

Details: All incidents are documented and reported to stakeholders.

Benefit: Provides accountability and a record for future reference and audits.

Compliance and Audit

Internal and External Audits:

Details: Regular audits are conducted to ensure compliance with ISO/IEC 27001:2013.

Benefit: Continuously improves the Information Security Management System (ISMS) and ensures ongoing compliance.

Continuous Improvement:

Details: Audit findings are used to enhance data protection measures.

Benefit: Keeps the ISMS effective and up-to-date with emerging threats.