The Ubicquia Security Program

A Foundation for a Smarter, Safer and More Connected World

Ubicquia has an engaged, evolving information security program to address security throughout the life of our products and across the entirety of our enterprise. We certify, validate, and test all our controls and provide multiple third-party attestations relating to such certification, validation, and testing. We strive to remove ambiguity and achieve trust through verification. Our goal is a robust program that empowers our customers to make informed decisions and provides our customers with peace of mind.

Highlighted through our ISO 27001 audit, our corporate Information Security Management System (ISMS) details a robust and continuously improving security program. We monitor the progress of our improvement through external auditors and an internal board to achieve and maintain a mature program throughout Ubicquia.

Certifications/Audits/Frameworks/Standards

ISO 27001/27002 -Audited	SOC2 Type 2 Planned for 2025
NIST 800-171	CTIA (IOT security) - Device Certification
NIST CSF	PCI SAQ-C
CMMC lvl 1 – Performed through SPRS	

Ubicquia Security Team

The Ubicquia security team has on average more than 9 years of experience and three security certifications. Whether studying it or practicing it, we love security. The team's goal is to build an information security program that addresses all business and product areas, controls attack surface, meets industry standards, and is effective in supporting Ubicquia's business objectives and customers.

Cloud Security

Ubicquia understands its role as a SaaS cloud service provider to its customers and, therefore, deploys substantial security measures to protect customer data. Such measures include policies, processes, people, and technologies to define and effectively implement Ubicquia's security controls. Customer data is secured via account configuration, access control using multi-factor authentication (MFA), auditing, and logging. Transmission of customer data to and from IoT devices is via MQTT using TLS 1.2+ protocol. All customer data is isolated from other customers by network segmentation and access control. Data at rest is secured using AES 256 database encryption. Furthermore, our government customer's data is hosted and secured in the AWS GovCloud to meet more stringent government security requirements.

Product Security

Ubicquia does not typically gather what would be considered PII and does not utilize what limited data that is gathered outside of required items to render services (sales, billing, email address/username). Telemetry data is gathered from all our devices and is controlled by our "Standard Terms and Conditions of Sale" which is owned by our legal department. It is available online at: Ubicquia-Standard- Terms-and-Conditions-of-Sale.pdf. Telemetry data is typically used to troubleshoot customer service issues and to aid us in improving our products and services. Data is stored within our AWS RDS databases, logically segmented for each customer, and encrypted at rest. Access to customer data is controlled through our

UbiVu® cloud-based asset management service's RBAC controls. Limited Ubicquia personnel will have access to the customer data.

- Advanced Encryption Standard (AES) 128/256-bit encryption.
- Trust M Security/Dedicated Security Controller for secure management of certifications for MQTTS and HTTPS (utilizing TLS 1.2+ encryption)
- Ubicquia's UbiCell® networked lighting controller is currently certified under Level 1 v1.2.3 of the Cellular Telecommunications and Internet Association (CTIA) IoT related security certification. The UbiCell networked lighting controller, along with Ubicquia's UbiHub® smart city platform, UbiHub access point, and UbiGrid™ intelligent distribution transformer monitor (DTM+), are targeted for CTIA Level 1 v2.1 certification in 2025.

Secure Software Development Life Cycle

Under its Secure Software Development Life Cycle (SDLC), Ubicquia segments development networks from production networks and secures development environments for system development/integration efforts. Our technology development and acquisition employ security measures during all phases of the SDLC to identify and appropriately remediate security and privacy-related risks. A SAST/SCA tool is currently in place that provides Static Application Security Testing (SAST) and Open Source Software (OSS) scanning. The tool is designed to help our application owners and development teams identify vulnerabilities in our software development process, including application code security and open source software (OSS) license compliance. The SDLC includes a formal change control process for all changes that affect Ubicquia's system components.

Communication Security

Encryption is an important part of Ubicquia's security strategy, helping to protect all communications, files, and other data. We use the highest recommended NIST Federal Information Processing Standards (FIPS) for encrypting Ubicquia and customer data, both at rest and in transit. We encrypt sensitive data while it is stored "at rest" (e.g., stored on a disk (including solid-state drives) or backup media).

Therefore, if an attacker obtains unauthorized access to the data, they won't be able to read the data because they don't have the necessary encryption keys. In addition, all data is encrypted while it is "in transit"(e.g., during transport over the Internet and across the cloud network between data centers). Ubicquia's system supports strong encryption protocols, such as TLS 1.2+, to secure the connections between customer IoT devices and cloud web services or application programming interfaces (APIs). Each customer's data is further logically separated from other customers' data at rest and in transit. Therefore, each customer's data is inaccessible to any other customer. The main backhaul communication for Ubicquia devices is the cellular LTE network. The cellular LTE network is segmented within the cellular service provider's network via an Access Point Name (APN). Once the APN data reaches the cellular service provider's infrastructure, it is sent to our AWS cloud service platform via a virtual private network (VPN). All traffic from each Ubicquia IoT device to our AWS cloud service platform uses TLS 1.2+ encryption. Such a communication path allows the IoT device to operate independently of a customer's IP network.

Cyber Assurance Program

Ubicquia's Cyber Assurance Program (CAP) supports the ISMS to protect and preserve the confidentiality, integrity, availability, and accountability of information assets through security assessments and audits. The CAP includes:

- Cybersecurity Tabletop Exercises: Annual exercises facilitated by Ubicquia's Cybersecurity team and including stakeholders to regularly evaluate and improve Ubicquia's cyber response process.
- Vulnerability Scanning: External and internal scanning to detect and remediate vulnerabilities in both cloud and product software environments and reduce the attack surface. External scanning is done independently by the Cybersecurity and Infrastructure Security Agency (CISA) to identify vulnerabilities that can be exploited by attackers. Internal scanning is performed using industry standard vulnerability management tools.
- Penetration Testing: Periodic testing to simulate various modern and legacy methods attackers may use to gain access to restricted systems or data. Findings are validated and mitigated/remediated to better protect assets and reduce the attack surface.
- Independent Audits: Ubicquia commissions independent third-party risk and compliance-based audits and assessments. Each audit or assessment results in the issuance of a certification, authorization, or other form of approval, which enables Ubicquia to measure the design and effectiveness of its security controls and continually mature the IISMS.

Incident Management

Incident response is a key aspect of Ubicquia's overall IISMS. We have a rigorous process for managing incidents led by the internal cybersecurity team in partnership with managed security service provider partners. Our incident response process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting the confidentiality, integrity, or availability of customer data. Ubicquia's incident response program is managed by its Cybersecurity team in partnership with cross-function stakeholders within the organization to tailor each response to the challenges presented by the particular incident. Following the successful remediation and resolution of an incident, the incident response team reviews both the cause(s) of the incident and Ubicquia's response, and then identifies key areas for improvement.

Logging and Monitoring

We monitor and analyze information gathered from applications, services, infrastructure, and endpoints. This information is collected in the form of event logs, audit logs, fault logs, administrator logs, and operator logs.
The logs are automatically monitored and analyzed through detections built into a Security Information Event Management (SIEM) system by identifying anomalies in the logs, such as unusual activity in our network or unauthorized attempts to access data.

Threat & Vulnerability Management

Ubicquia is continuously working to reduce the severity and frequency of vulnerabilities across its products, services, and infrastructure through our Threat & Vulnerability Management (TVM) program. The TVM program monitors for new security threats and vulnerabilities to identify, track, and remediate across applications and infrastructure.

Vulnerabilities are identified through different methods, such as automated scanners, internal security reviews, and penetration testing assessments. Once a vulnerability has been identified, the Cybersecurity team logs it, prioritizes it accordingly, and assigns an owner for remediation. The team tracks each issue and follows up frequently until remediation is completed.

Third Party Vendor Risk Management

Ubicquia evaluates and qualifies our vendors based on our Third-Party Risk Management policy. New vendors are onboarded after evaluating their processes for delivering services to Ubicquia and performing risk assessment. Risks identified through the process are flagged and discussed with the vendor for mitigation or remediation. All vendors must adhere to the cybersecurity commitments we have made to our customers. We continue to assess the cyber risk of our vendors via subsequent reviews either at contract renewal or annually depending on the risk level of
the engagement.

About Ubicquia

Ubicquia makes critical infrastructure intelligent to improve energy efficiency, grid resilience, and asset management for utilities and municipalities. Harnessing the power of advanced analytics and AI, Ubicquia processes 2 billion data points daily, providing insights to optimize the operations of streetlights, distribution transformers, and utility poles. Its platforms are deployed in more than 800 cities and integrated with leading streetlight, transformer, and public safety solutions.

To Learn More

Visit us at www.ubicquia.com or email us at info@ubicquia.com

ubicquia