CYBERSECURITY AND DATA PRIVACY SHEET

C•CURE Cloud

A comprehensive approach to keeping your business safe

Gain peace of mind with cyber-resilient systems and solutions which protect your data. Security is designed into all Johnson Controls products, hardware, hosted services and software. The C•CURE Cloud security features listed below enable you to unlock the value in your building knowing that your systems are protected.

Data Encryption
AES-256 encryption protects data-at-rest and TLS-1.3 for data in transit, also building data is sent from site to cloud, encapsulated within a Zero-trust Host Identity Protocol (HIP) encrypted tunnel.

Role-based Access Control (RBAC)
Assign permissions according to authorized roles

Validated Authentication
Multi-Factor Authentication (MFA) enhances access control by requiring additional proof of identity

Zero-Trust Cloud Connectivity
Devices communicate over the software-defined overlay network using zero-trust policy-managed authorizations

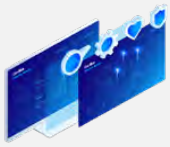
High Availability
Fast recovery from a Virtual Machine (VM) or Availability Zone (AZ) outage

Vulnerability Monitoring
Environment is continuously monitored for security issues or mis-configurations

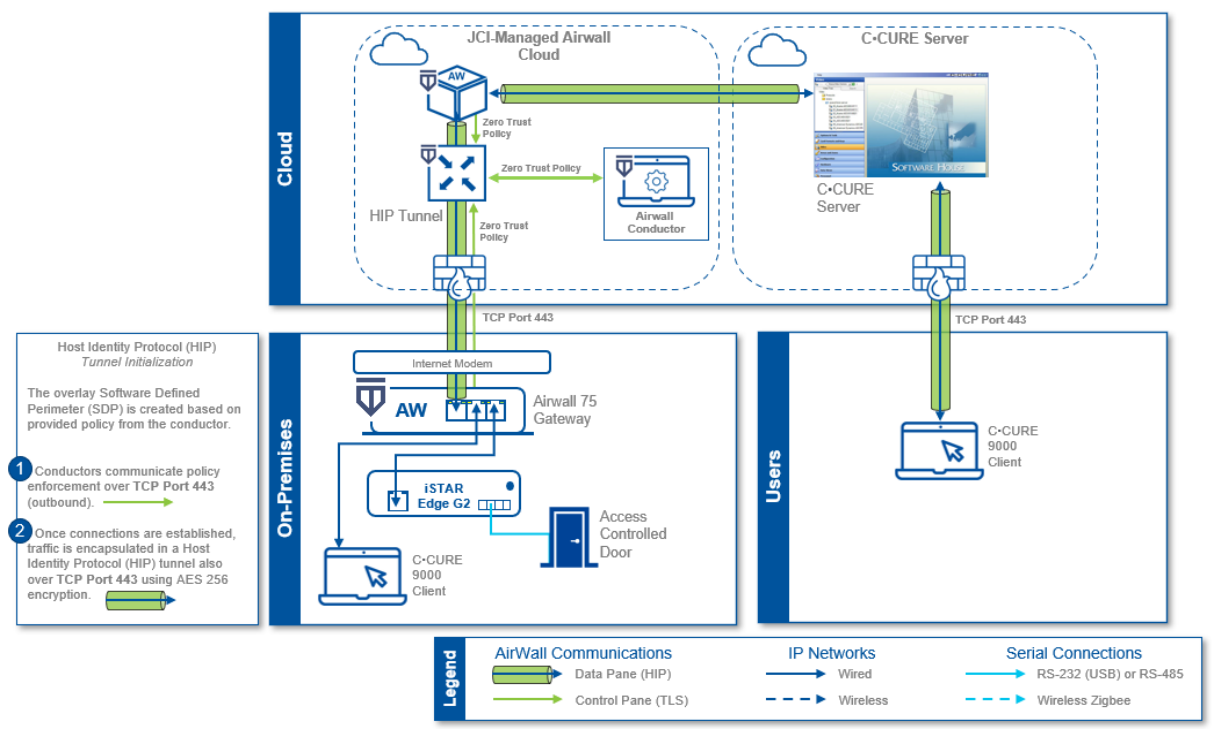
About C•CURE Cloud

C•CURE Cloud is a premier cloud solution tailored for medium to large businesses transitioning from on-premise C•CURE Server and Software to a fully managed cloud environment. Built on Virtual Machine (VM) instances, this purposed-driven platform leverages IoT and AI technologies to align with your specific goals and maximize your investments. With C•CURE Cloud, you can design your smart infrastructure one use case at a time, ensuring a customized approach to meet your unique needs.

Learn more here



C•CURE Cloud Architectural and Data Flow



The specifics of data flow will vary based on the components selected by the customer and the implementation of the solution within the facility.

ISASecure® Security Development Lifecycle Assurance (SDLA) Certified

All Johnson Controls global development locations comply with this security lifecycle development certificationconforming with ISA/IEC 62443-4-1 and encompassing all associated brands. This certification reinforces our customercommitment to provide cyber-resilient solutions that follow best-in-class industry practices.

ISASecure® Security Development Lifecycle Assurance (SDLA) program certified

Data Privacy

Johnson Controls has a Global Privacy Office and a Global Privacy Program, involved at the beginning and throughout the design and development of our processes, activities, products, services and solutions, in accordance with internationally accepted principles of Privacy by Design. The Johnson Controls Privacy Program is led by our privacy experts and designed with the most stringent global privacy and data protection laws. In addition to product-related information provided in this section please visit www.johnsoncontrols.com/trust-center/privacy for more details on our Global Privacy Program.

a. Personal data processing details of C•CURE Cloud

See below for details on each category of personal data processed by C•CURE Cloud, types of personal data within each category, and the purpose of processing each type:

Personal Data Category	Type of Personal Data	Purpose of Processing
User and account information	• First name, middle name, last name • User login ID • User email ID • Phone number (optional) • Department • Business unit • Work location • Login Data	• Required for user identification • Required for user notifications • Required for audit records of actions taken by specific users for security and compliance
Facility access details	• First name, middle name, last name • Phone number optional • License plate • Department • Personnel type (employees, visitor , contractor , etc.) • Badge ID • PIN number (associated with the badge) • Business address • Profile image • Badge in and badge out time • Business unit • Work location • Biometric data (optional, for two factors authenticationD	• Required for visitors and occupants identification and facility access assigned • Required for audit records of actions taken by specific users for security and compliance

b. Data retention and deletion

Johnson Controls has a Global Records Management Program, which includes a Global Records Retention Policy and procedures. The purpose of our Global Records Management Program is to detail the responsibilities and working instructions necessary for the use, maintenance, retention, or deletion of data Johnson Controls is processing. The Global Records Management Program applies to all worldwide locations and legal entities controlled by Johnson Controls.

When Johnson Controls processes personal data on behalf of a customer, or when products are operating on customer site, to the extend provided by a product's functionalities and upon a system's configuration, Customers may access such data and delete it at any time on their own. The default retention periods as predefined by Johnson Controls apply. See the below table for the default retention periods applied to C•CURE Cloud.

If, during the 90 days following the end of a subscription, Johnson Controls received from customer a request to export customer's personal data, Johnson Controls will provide customer an export of its personal data in a structured commonly used machine-readable format as reasonably determined by Johnson Controls. Such request must be made to the JCI Digital Customer Support email currently at **CCURECloud-PSG@jci.com.** If not already deleted by customer using available internal product deletion features, customer's personal data will be deleted after such 90-day period or as otherwise agreed or provided below. During any retention period, the provisions of the underlying agreement that are applicable to the retention and product of a customer's personal data continue to apply.

Default retention periods for customer personal data are as set forth in the table below:

Sub-Processor	Type of Personal Data	Purpose of Processing
• First name, middle name, last name • User login ID • User email ID • Phone number (optional) • Department • Business unit • Work location • Login Data	For the subscription period + 90 days, except for journal data which is retained for the time period of no longer than 25 months upon creation. Journal data is non-static data referred to user's and facility access' events and operations, such as e.g. badging, systems's user activities, etc.	• Required for user identification • Required for user notifications • Required for audit records of actions taken by specific users for security and compliance
Facility access details • First name, middle name, last name • Phone number optional • License plate • Department • Personnel type (employees, visitor , contractor , etc.) • Badge ID • PIN number (associated with the badge) • Business address • Profile image • Badge in and badge out time • Business unit • Work location • Biometric data (optional, for two factors authenticationD	For the subscription period +90 days, except for journal data, which is retained for the time period of no longer than 25 months upon creation. Journal data is non - static data referred to user's and facility access' events and operations, such as e.g. badging, systems's user activities, etc.	• Required for visitors and occupants identification and facility access assigned • Required for audit records of actions taken by specific users for security and compliance

c. Sub-processors for C•CURE Cloud

Please see below the list of current sub-processors utilized for C•CURE Cloud Services

Sub-Processor	Service Type	Location of Data Centers
Amazon Web Services	Third-party cloud hosting	Based on customer's location: US East US West Canada Central

d. Cross-border data transfers

Many countries and jurisdictions have laws governing the transfer of personal data. As a multinational organization, Johnson Controls has substatial experience in dealing with cross-border transfer issues and restrictions. When Johnson Controls processes personal data for our own purposes or on behalf of a customer, we utilize the following transfer mechanisms which can assist our customers:

Binding Corporate Rules (BCRs)	The Johnson Controls BCRs are designed to ensure an adequate level of protection for personal data no matter where in the world it is processed by Johnson Controls. With respect to the European Union (EU), the Johnson Controls BCRs have been specifically approved by the EU Data Protection Authorities (DPAs) for transfer of EU personal data globally within Johnson Controls.
Asia-Pacific Economic Cooperation Cross-Border Privacy Rules (APECCBPR)	The CBPR is a government-backed privacy certification which demonstrates that Johnson Controls complies with internationally recognized data privacy protections and is the framework approved for the transfer for personal data by Johnson Controls between participating APEC member economies: the United States, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei and the Philippines.

Asia-Pacific Economic Cooperation Privacy Recognition for Processors (APEC PRP)	The PRP is a government-backed privacy certification that enables Johnson Controls to demonstrate to customers our accredited enterprise-wide Privacy Program and to transfer data processed on behalf of our customers (including our cloud solutions) between the United States, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei, and the Philippines. Please see the PRP Directory and the Johnson Controls PRP TRUST e-validation page for more information.
EU Standard Contractual Clauses (SCCs)	Johnson Controls incorporates the EU's approved standard contractual clauses, also referred to as the "Model Contract", into the Johnson Controls Data Protection Agreement located at www.johnsoncontrols.com/dpa to afford the contractual protection under the SCCs to your customers.
US Data Privacy Framework	Johnson Controls is certified under US Data Privacy Framework for transfers of personal data from the European Union (EU), United Kingdom (UK), and Switzerland.

Please note that this document is for customer guidance purposes only, is not legal advice and is subject to changes from time to time due to modifications of our solutions. Johnson Controls is not a law firm and does not provide legal advice. While Johnson Controls products and solutions are designed for use in compliance with applicable law implementation and deployment of Johnson Controls products and solutions should be reviewed by appropriate customer advisors and stakeholders for such compliance.

We combine our critical focus on cybersecurity and privacy with digital innovation and building expertise to deliver smart building solutions.

To learn more, please visit our website at **www.johnsoncontrols.com/trust-center** or contact us at **TrustCenter@jci.com.**

Visit **johnsoncontrols.com** or follow us **@johnsoncontrols**

DS2403001 | GPS0057-CE-EN Rev A 2025-01-29

Johnson Controls