Johnson Controls

Cybersecurity and data privacy sheet

Maintaining chiller health through advanced analytics and insights

Securing chiller performance

1. Solution overview

OpenBlue Services for Optimizing Chiller Performance feature tailored, AI-powered technology that enables remote diagnostics, predictive maintenance, compliance monitoring, advanced risk assessments and more.

At Johnson Controls, we harness innovation to create connected solutions that maintain the health of critical equipment such as chillers, ensuring they last longer and perform better with our best-practice optimization strategies.

Increase uptime and reliability

Increase energy savings and sustainability

Reduce total cost of ownership

Increase staff efficiency

2. General cybersecurity features

Security is designed into all our products – Johnson Controls hardware, software and hosted services.

Our cybersecurity and data privacy practices are aimed at addressing security holistically for our customers, products and enterprise.

Encrypted communications: Chiller data is sent encrypted from the Connected Equipment Gateway (CEG) to the cloud using Transport Layer Security (TLS)

Zero-trust connection: All messages are sent to cloud services using the tempered zero-trust solution which further encapsulates all traffic from the site using Host Identity Protocol (HIP)

Zero-trust policy-managed authorizations: Only a single path is permitted between the CEG and cloud services

Hidden IP addresses: The IP address for the CEG is not exposed to the internet

Outbound communications only: Only two outbound ports are required to initiate CEG site-to-cloud data exchange

Remote updates: CEG periodically requests security updates from the authenticated cloud service. Updates are downloaded and installed automatically

Forced password change: Default user account passwords must be changed when commissioning the CEG

Forced Wi-Fi setting change: When optional Wi-Fi is used, default Wi-Fi IDs and passphrases must be changed during initial configuration

Read-only chiller communications: When exclusively using YORK® or Wuxi Chillers, a dedicated port will ignore all BACnet commands

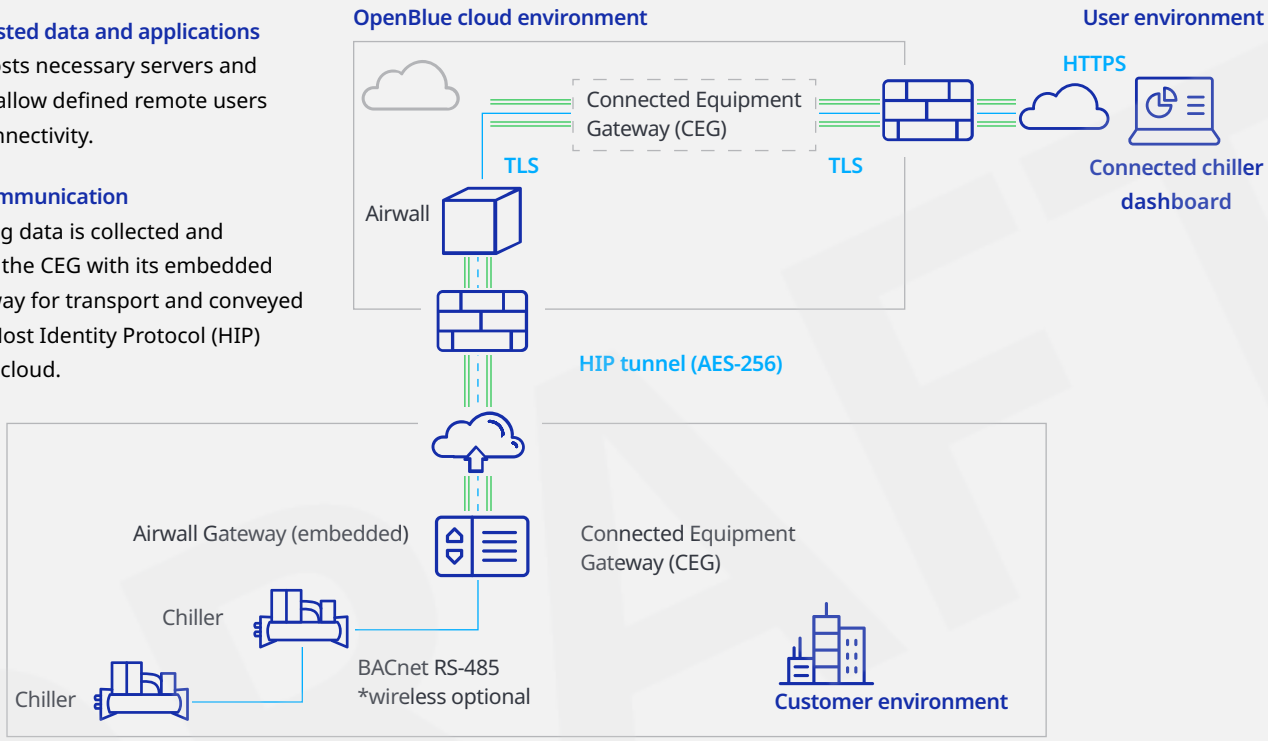
Cybersecurity and data privacy sheet

3. Architectural and data flow

The specifics of this flow depend on the components chosen by our customer and how we implement our solution in their facility.

OpenBlue hosted data and applications
CEG Cloud hosts necessary servers and resources to allow defined remote users and client connectivity.

Zero-trust communication
Smart building data is collected and packaged via the CEG with its embedded Airwall Gateway for transport and conveyed securely via Host Identity Protocol (HIP) tunnel to the cloud.



4. ISASecure® Security Development Lifecycle Assurance (SDLA) program certified

All Johnson Controls global development locations were found to be in compliance with this security lifecycle development certification conforming with ISA/IEC 62443-4-1 and encompassing all associated brands. This certification reinforces our commitment to our customer to provide cyber-resilient solutions that follow best-in-class industry practices.

5. ISASecure Component Security Assurance (CSA) certification - an industry first

Johnson Controls is the industry's first to receive ISA/IEC 62443 CSA certification of YK/YZ Centrifugal Chiller achieved on September 15, 2021. This chiller is a primary play for data centers around the globe. Our organization continues to be future-focused and strives to achieve further accolades in the industry.

6. 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/privacy-center for more details on our Global Privacy Program.

Cybersecurity and data privacy sheet

a. Personal data processing details of the connected chiller dashboard

See below details on each category of personal data processed by the connected chiller dashboard, types of personal data within each category, and the purpose of processing each type:

Personal data category	Types of personal data	Purpose of processing
User and account information	• First name • User login ID • User email ID • Business contact number	• Required to run an active subscription • Required for licensing • Required for user notifications

b. Data retention and deletion

Johnson Controls has a Global Records Management Program, which includes global records retention 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 personal data Johnson Controls is processing, and to assign appropriate responsibilities to the right individuals. 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 our products are operating on customer site, to the extent provided by the product's functionalities and upon the system's configuration, the customer may access such data and delete 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 the connected chiller dashboard.

Prior to the end of a subscription, Customer may export its personal data using the available products internal export features. If, during the 90 days following the end of a subscription, Johnson Controls receives 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, BE-ConnectedOfferingsSupport@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. During any retention period, the provisions of the underlying agreement that are applicable to the retention and production of Customer's personal data continue to apply.

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

Data category	Types of personal data	Purpose of processing
User and account information: • First name, middle name, last name • User login ID • User email ID • Business contact number	For the period of active subscription + 90 days	• Required to run an active subscription • Required for licensing • Required for user notifications

c. Sub-processors for the connected chiller dashboard

Please see below the list of current sub-processors utilized to provide the connected chiller dashboard:

Sub-processor	Personal data	Service type	Location of data center	Security assurance
Microsoft Azure Cloud	• First name, middle name, last name • User login ID • User email ID • Business contact number	Third-party cloud hosting	United States	• For information regarding Microsoft Azure see https://www.microsoft.com/en-ie/trust-center/compliance/compliance-overview • Audit reports

Cybersecurity and data privacy sheet

d. Cross-border data transfers

Many countries and jurisdictions have laws governing the transfer of personal data. As a multinational organization, Johnson Controls has substantial 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 of 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 (APEC CBPR)	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 of 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, Republic of Korea, Australia, Chinese Taipei and the Philippines. Please see the PRP Directory and the Johnson Controls PRP TRUSTe 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 our customers.
US Data Privacy Framework (DPF)	Johnson Controls is certified under the US Data Privacy Framework for transfers of personal data from the European Union (EU), United Kingdom (UK) and Switzerland.