CYBERSECURITY AND DATA PRIVACY SHEET

OpenBlue Enterprise Manager

With **OpenBlue Enterprise Manager** we deliver real-time data visibility across assets, people and processes, empowering our customers to drive intelligent and proactive operations. Our smart building platform provides a gateway to the live activity of a building to create the following outcomes:

- Energy Efficiency and Sustainability
- Space, Wellbeing and Productivity
- Operational Efficiency and Equipment Optimization
- Security, Safety and Compliance

A comprehensive approach to keeping your business safe

Gain peace of mind with cyber-resilient systems and solutions which protect your data for use within this cloud application. Security is designed into all Johnson Controls products, hardware, hosted services and software. The OpenBlue Enterprise Manager security features listed below enable you to unlock the value in your building knowing that your systems are protected.

Data-at-rest protection
AES-256 encryption protects data-at-rest

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

Network security
Web Application Firewall (WAF) protects against sophisticated attacks

Role-based access control (RBAC)
Assign permissions according to authorized roles

Zero-trust cloud architecture
OpenBlue from site-to-cloud and within applies zero-trust management for enhanced data protection

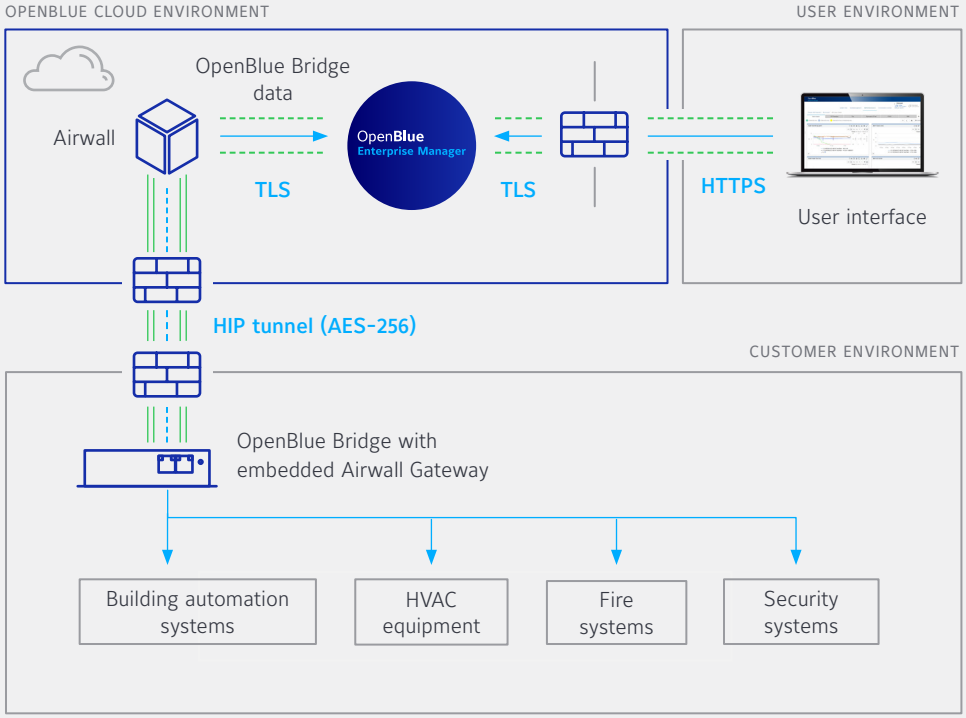
Regular vulnerability assessments
The OpenBlue environment is continuously monitored for cyber events using automated tools

How OpenBlue Enterprise Manager protects your people and assets

Architectural environment is representative of OpenBlue Bridge with embedded Airwall Gateway

Cloud
OpenBlue hosted data and applications.

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



ISASecure® Security Development Lifecycle Assurance (SDLA) certified
All Johnson Controls global development locations comply with this security lifecycle development certification conforming with ISA/IEC 62443-4-1 and encompassing all associated brands. This certification reinforces our customer commitment to provide cyber-resilient solutions that follow best-in-class industry practices.

SOC 2 Type II Report Compliance
A SOC 2 Type II audit is an evaluation of an organization's information systems and controls based on the criteria outlined in the Trust Service Criteria. It focuses on security, availability, processing integrity, confidentiality and privacy. The "Type II" indicates that the audit covers a specified time period (usually a minimum of six months), to assess the effectiveness of the controls in place.

ISO27001 Certification
ISO/IEC 27001:2013 is an international standard that specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security Management System (ISMS) within the context of the organization's overall business risks. The standard provides a systematic approach to managing sensitive information ensuring its confidentiality, integrity and availability.

ISASecure® Security Development Lifecycle Assurance (SDLA) program certified

SOC 2 Type II Report Compliance*

ISO27001 Certification*

* The US instance has successfully undergone SOC 2 Type II Audit and ISO/IEC 27001:2013 Certification. International instances have substantially similar controls and protocols.

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 OpenBlue Enterprise Manager

See below details on each category of personal data processed by OpenBlue Enterprise Manager, types of personal data within each category and the purpose of processing each type:

Personal data category	Type of personal data	Purpose of processing
Work-related identification details	· Full name · Full email address · User ID · Phone number · Preferred language · Picture (optional)	Account management

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 extent 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 OpenBlue Enterprise Manager.

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 openbluetechnicalsupport@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 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:

Personal data category	Retention period	Reason for retention
Work-related identification details: · Full name · Full email address · User ID · Preferred language · Phone number · Picture (optional)	For the subscription period +90 days	Account management

c. Sub-processors for OpenBlue Enterprise Manager

Please see below the list of current sub-processors utilized for OpenBlue Enterprise Manager:

Service type	Sub-processor	Location of data centers
Cloud hosting service	Microsoft Azure (upon customer's choice)	United States, Canada, EU (Germany), Singapore
Cloud hosting service	Alibaba Cloud (upon customer's choice)	Saudi Arabia
Data hosting and computing service	Snowflake	Azure US, Azure EU, Azure Singapore

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 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 (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.
Data hosting and computing service	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.

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/cyber-solutions** or contact us at **productsecurity@jci.com**.

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

© 2024 Johnson Controls. All rights reserved.
OB2412001 | GPS0050-CE-EN Rev B 2024-12-16

Johnson Controls