Cybersecurity practices for a digitally connected world

At Johnson Controls, we provide digitally connected and resilient solutions to help customers achieve their business outcomes and optimize their smart building experience. As a trusted partner, we have a shared responsibility to help power and protect their mission from cyber threats by ensuring cybersecurity risks are managed throughout the lifecycle of the solutions we develop, support and service. Our security practices are reinforced through policies, standards, guidelines and technology solutions. This approach spans our entire product portfolio and enterprise information environment, so that we can address cybersecurity holistically for our customers.

For the customer

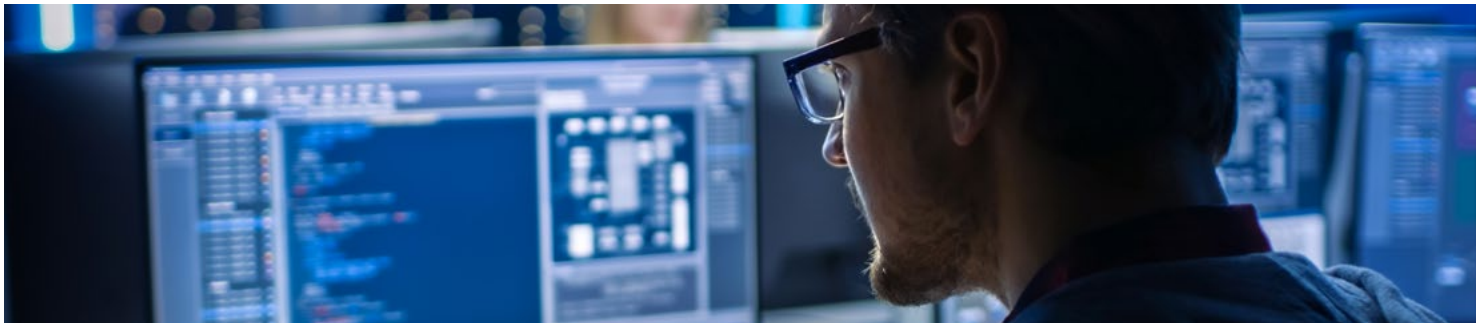
Our customers are increasingly concerned about cybersecurity and privacy and Johnson Controls makes it a top priority to actively manage risks to customer information and product operations. We have dedicated organizations governing product security, information security, and data privacy. These organizations work together to deliver high-quality and consistent cybersecurity and data privacy support in a way that meets the unique mission and technology needs of each customer.

Data privacy

Data privacy practices are managed across our enterprise functions and includes activities that support product sales, operations and servicing.

Johnson Controls enterprise environments are TRUSTe certified. TRUSTe Certification ensures consistency with the TrustArc framework to help demonstrate privacy compliance and data governance in accordance with globally recognized laws and regulatory standards such as:

- EU General Data Protection Regulation (GDPR)
- ISO 27001
- U.S. Health Insurance Portability and Accountability Act (HIPAA)
- OECD Privacy Guidelines
- APEC Privacy Framework including APEC Cross Border Privacy Rules (CBPR) Seal
- Privacy Recognition for Processors (PRP) Seal



Enterprise

Johnson Controls protects the digital environments that run our business systems, support development, and host customer data and applications. This is led globally by the Chief Information Security Officer (CISO).

At Johnson Controls, our unified security control framework is applied across the enterprise and is derived from industry standards such as:

- **National Institute of Standards and Technology (NIST) 800-53**
- **International Organization for Standardization (ISO) 27001**
- **Payment Card Industry Data Security Standard (PCI DSS)**

Product

Johnson Controls designs cybersecurity into our commercial product offerings and endeavors to protect those solutions (including software, hardware and hosted solutions) throughout the product lifecycle. Our secure product practices include the design, sourcing, development, deployment, support and retirement of products. All new Johnson Controls commercial products are developed under the governance of our cybersecurity policies. This is led globally by the Chief Product Security Officer (CPSO).

Secure Development Lifecycle

Johnson Controls is ISASecure Secure Development Lifecycle Assurance (SDLA) certified. Johnson Controls branded solutions are within the scope of this certification.

- **Secure by design –** Products adhere to established criteria and include security controls for the intended operational environment in compliance with applicable standards and regulations.
- **Security testing –** Johnson Controls products undergo internal and external assurance testing, including vulnerability scans and penetration tests as required.
- **Supply chain risk management –** Johnson Controls validates that third-party suppliers of essential products, components and technology solutions meet our security requirements.
- **Lifecycle risk management –** Products are developed and solutions are deployed in a way that helps our customer meet their compliance requirements.

Cloud solutions – OpenBlue and others

OpenBlue is a complete suite of connected smart building solutions, from edge to cloud. OpenBlue and other cloud-based solutions from Johnson Controls hosted in Microsoft Azure, Google Cloud or Amazon Web Services are protected environments that conform to industry-recognized standards, such as:

- **ISO 27001 – Information Security**
- **ISO 27017 – Information Security for Cloud Services**
- **ISO 27018 – Code of Practice for Personal Data in the Cloud**
- **SOC 1, 2, 3 – Service Organization Controls – Safeguarding Confidentiality and Privacy of Information Stored and Processed in the Cloud**

Additional security compliance information for these environments is available at:

- **Google Cloud compliance website:** **https://cloud.google.com/security/compliance/offerings#/**
- **Microsoft Azure compliance website:** **https://docs.microsoft.com/en-us/compliance/regulatory/offering-home**
- **Amazon Web Services compliance website:** **https://aws.amazon.com/compliance/programs/**

Data protection

When processing customer information, we have data protection controls in place to strictly limit access to authorized personnel. Sharing of data with third parties is defined by functionality and terms associated with each solution and occurs when authorized by the data owner.

Incident response

- Johnson Controls activates its security incident response process and adheres to disciplined operating procedures when responding to a security incident or breach.
- A tiered escalation and coordination process is followed that includes initial triage, severity determination, and customer notification.

Vulnerability management

Johnson Controls uses the Common Vulnerability Scoring System (CVSS) to inform security vulnerability management activities. Johnson Controls policy requires remediation of all critical and high vulnerabilities.

- **Threat intelligence –** Our Product Threat Intelligence Program actively monitors various security vulnerability feeds and submits validated issues to product teams for analysis and action. Advisories and product updates are provided as required.
- **Coordinated disclosure –** Johnson Controls practices coordinated vulnerability disclosure as a MITRE CVE® (Common Vulnerabilities and Exposures) Numbering Authority (CNA). As a CNA, the Johnson Controls Global Product Security organization has the ability to self-report our product vulnerabilities to the publicly accessible National Vulnerabilities Database (https://nvd.nist.gov). This capability is incorporated into our Product Security Incident Response (PSIR) and vulnerability management processes.

In addition, notification is provided to the United States Cybersecurity and Infrastructure Security Agency when we publish a CVE.

Disaster recovery

Johnson Controls has disaster recovery and business continuity plans in place to minimize disruption and recover from a cybersecurity incident.

Training

Our Cybersecurity Training and Awareness Policy requires that all Johnson Controls employees and contingent workers with login credentials participate in mandatory cybersecurity training.

Cybersecurity training is integrated into our Product Security Program, which requires all product developers and engineers to complete the designated cybersecurity training curriculum for their role.

Outreach/memberships

Johnson Controls actively participates in cybersecurity community initiatives and is a key contributor in defining security standards and best practices for smart buildings. We maintain membership with several security organizations including, but not limited to, the following:

- **ISAGCA – Founding member of the International Society of Automation's (ISA) Global Cybersecurity Alliance (GCA)**
- **ISCI – International Society of Automation's (ISA) Security Compliance Institute**
- **FIRST – Full member of Forum of Incident Response and Security Teams (FIRST)**
- **MITRE – Common Vulnerabilities and Exposures (CVE) Numbering Authority**

We combine our critical focus on cybersecurity and privacy with digital innovation and building expertise to power your mission.

Johnson Controls

Johnson Controls is a global diversified technology and multi industrial leader serving a wide range of customers in more than 150 countries. Our 120,000 employees create intelligent buildings, efficient energy solutions, integrated infrastructure and next generation transportation systems that work seamlessly together to deliver on the promise of smart cities and communities. Our commitment to sustainability dates back to our roots in 1885, with the invention of the first electric room thermostat. We are committed to helping our customers win and creating greater value for all of our stakeholders through strategic focus on our buildings and energy growth platforms.

For additional information, please visit **www.johnsoncontrols.com/cyber-solutions** or follow us on Facebook, Twitter, and LinkedIn.

GPS0020-CE-20210625-EN

The power behind **your mission**

Johnson Controls