Security Practices

GPS0009-CE-EN
Rev D
Revised 2023-05-12

The power behind **your mission**

Johnson Controls

Content

1	Introduction	4
2	Security organizations	5
2.1.0	Enterprise Information Security Program	6
2.1.1	Key capabilities of the Information Security Program	6
2.2.0	Product Security Program	7
2.2.1	Key capabilities of the Product Security Program	7
2.3.0	Dedicated security professionals	7
3	Security policies	8
3.1.0	Enterprise information security policies and standards	9
3.1.1	Management control policies	9
3.1.2	Operational controls policies coverage	9
3.1.3	Technical controls coverage	9
3.2.0	Product security policies	9
3.2.1	Product security policies	9
3.3.0	Policy-based security practices	9
4	Human resource security	10
4.1.0	Background screening	10
4.2.0	Employee separation	10
5	Security training	11
5.1.0	Cybersecurity training – All employees	12
6	Secure product development	13
6.1.0	Secure development lifecycle	14
6.2.0	Product development requirements	14
6.3.0	Security training – Product development	14
6.4.0	Baseline product security requirements and coding practices	15
6.5.0	Product security testing practices	15
6.6.0	Supply chain management practices	16
6.7.0	Security integration	16
6.8.0	Security checkpoints	16
6.9.0	Security roles	16

7	Vulnerability management	17
7.1.0	Product vulnerability management requirements	18
7.2.0	Vulnerability scoring	18
7.3.0	Product threat intelligence	18
7.4.0	Product Security Advisories	18
7.5.0	Additional product vulnerability disclosure channels	19
7.5.1	The National Vulnerabilities Database	19
7.5.2	The United States Department of Homeland Security Industrial Control System	19
7.6.0	Enterprise vulnerability management	19
8	Incident response	20
8.1.0	Enterprise security incident response	21
8.2.0	Product security incident response	21
8.3.0	Product security incident response readiness	21
8.4.0	Privacy incident response	21
8.5.0	Customer notification	21
9	Enterprise security practices	22
9.1.0	Risk management	23
9.2.0	Business continuity and disaster recovery	23
9.3.0	Business continuity	23
9.4.0	Disaster recovery	23
9.5.0	Device management	24
9.5.1	Computing and mobile device security	24
9.5.2	Software update and patching	24
10	Security memberships	25
10.1.0	ISA Security Compliance Institute (ISCI)	26
10.2.0	ISAGCA	26
10.3.0	FIRST	26
10.4.0	MITRE	26
11	Audit, security standards and compliance	27
11.1.0	Auditing	28
11.2.0	ISASecure® Secure Development Lifecycle Assurance Certification (SDLA)	28
12	Summary	29

1 Introduction

We at Johnson Controls follow a security practice to ensure that cybersecurity is addressed throughout the lifecycle of the solutions we develop, support and service. This document describes an overview of Johnson Controls security practices. Our practices are aimed at addressing security holistically for our customers, products and enterprise.

The practices outlined address Johnson Controls branded products and solutions. For third-party non-Johnson Controls branded products and solutions consult with the respective supplier.

2 Security organizations

Cybersecurity is a top priority for Johnson Controls and is managed by our dedicated Global Information Security (GIS) and Global Product Security (GPS) organizations.

Johnson Controls promotes a collaborative approach to security governance and management. Our GIS and GPS organizations partner with each other in addition to other internal organizations to ensure our actions are tightly coordinated. Such other internal organizations include:

- Corporate Governance and Compliance
- Enterprise Risk Management
- Global Privacy Office
- Internal Audit
- Legal
- Procurement

Together, these organizations deliver on the Johnson Controls commitment to security, privacy and ethics.

2.1.0 Enterprise Information Security Program

Enterprise systems and endpoints managed by Johnson Controls Global Information Security (GIS) are maintained to protect the integrity of our customers', partners' and employees' information against unauthorized disclosure, alteration, access and unlawful destruction.

Our information 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)

In addition to regulatory requirements and global data protection laws such as:

- Sarbanes-Oxley
- European Union's General Data Protection Regulation (GDPR)

Johnson Controls honors the privacy and confidentiality of individuals and business partners.

2.1.1 Key capabilities of the Information Security Program

Here you can find information on the key capabilities of the Enterprise Information Security Program.

2.1.1.2 Policy Governance and Cybersecurity

Strategy and governance
- Information security policy and standards governance
- Security awareness and training
- Security architecture
- Security metrics, analytics, and reporting

Security engineering
- Security platform engineering
- Security automation and integration

Security operations
- Vulnerability management
- Incident management
- Threat automation and analysis
- Customer cloud monitoring

IT Risk Management and compliance
- IT Audit monitoring
- IT Risk assessments (including third party risk)
- T/Security regulatory and compliance assurance

Information protection
- Data loss prevention
- Insider threat management

2.2.0 Product Security Program

Johnson Controls endeavors to provide its customers with secure products, (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.
The Global Product Security (GPS) team operates autonomously from product development to provide independent cybersecurity oversight.

2.2.1 Key capabilities of the Product Security Program

Governance
- Governance and risk management
- Security policies and standards
- Secure design requirements and features
- Secure development and testing
- Supplier risk management
- Vulnerability assessment and penetration testing
- Security training and awareness
- Security metrics and compliance reporting

Engineering
Johnson Controls Security Practices

Integration
- Security tool integration
- Tool lifecycle support
- Public key infrastructure – Digital certificate management

Operations
- Product security incident response
- Coordinated vulnerability disclosure
- Threat intelligence and hunting

Experience
- Customer experience
- Customer inquiries and audits
- External communications

Certifications
- Multi-Level Protection Scheme (MLPS)
- ISO 27001 Controls Monitoring
- SOC 2 Controls Monitoring
- ISA/IEC 62443 Secure Development Lifecycle and Component

2.3.0 Dedicated security professionals

Our security organizations are comprised of certified cybersecurity professionals, for example, Certified Information Systems Security Professional (CISSP), who use the latest recognized industry standards and practices to validate designs and implementations.

3 Security policies

The security policy framework of Johnson Controls defines an overarching set of governing security practices for the enterprise. Policies are supported by standards, procedures and guidelines which provide details on expected behaviors and actions that protect the company against cybersecurity risks.

Security policies for product and enterprise are reviewed periodically and revised based on material changes in Johnson Controls business strategy, computing/ technology environment and applicable regulatory or compliance requirements.

3.1.0 Enterprise information security policies and standards

Enterprise information security policies and standards address management controls, operational controls and technical controls:

3.1.1 Management control policies

- Enterprise Information Security Program
- Acceptable use of computing resources
- Information security awareness
- Human resource (HR) security
- Third-party risk management
- IT regulatory and compliance

3.1.2 Operational controls policies coverage

- Information classification and protection
- IT asset management
- Application security
- Endpoint protection
- Vulnerability and patch management
- Incident response management
- Disaster recovery

3.1.3 Technical controls coverage

- Access control security
- Encryption and key management
- Network and communications security
- Configuration management
- Identity and authentication management

3.2.0 Product security policies

Johnson Controls product security policies govern products and address all phases of the product lifecycle and includes the application of a Secure Development Lifecycle (SDLC).

3.2.1 Product security policies

- Secure Product Development
- Secure Product Supply Chains
- Secure Product Operations & Servicing

3.3.0 Policy-based security practices

Johnson Controls security practices are defined by or derived from our security policies as with supporting standards, guidelines and processes. In the following sections we will highlight several practices which are commonly required as part of supplier validation and contribute to our cybersecurity maturity.

4 Human resource security

This section describes our practices surrounding human resource security.

4.1.0 Background screening

The Johnson Controls human resources organization requires background screening for employment. The depth of screening and information shared align with regional laws and the requirements of the job role.

4.2.0 Employee separation

Employee access rights are removed upon termination.

5 Security training

This section describes our security training practices.

5.1.0 Cybersecurity training - All employees

The Johnson Controls Cybersecurity Training and Training Standard states that all employees with login credentials and a company email address are required to complete assigned cybersecurity training.

The Cybersecurity Training and Awareness Program supports continual learning throughout an employee's tenure, delivering cybersecurity awareness materials throughout the year through a variety of Company communications and training channels. This includes onboarding, role-based, and policy/ compliance related education, to ensure employees are clear on their role in protecting company systems and data. Advanced training may be required for certain business functions, roles or responsibilities.

Cybersecurity Training and Awareness program content covers, but is not limited to, the following areas:

- Acceptable use of company computing and information assets
- Identifying and reporting phishing (and other forms of social engineering)
- Information security and policy governance essentials
- Role-based cybersecurity awareness education
- Ethics and compliance
- Workplace safety
- Records and information management

6 Secure product development

This section describes our secure product development practices.

6.1.0 Secure Development Lifecycle

Johnson Controls Building Technologies and Solutions Global Products businesses follow the Microsoft Security Development Lifecycle (M-SDL) to help proactively identify and remediate vulnerabilities in product software prior to product release. Product security baseline requirements are derived from established cybersecurity standards for example, OWASP, NIST SP 800-53r5, ISA/IEC 62443, UFC 4-010-06, tailored for operational technology domain and address 14 core threat categories, including: authentication, access control, session management, data protection and malicious input handling. Product development teams adhere to an internal technical process called Design for Security, and perform various security testing measures, including, in some cases, having internal or external black box penetration testing performed. Global Products also has a product security incident response (PSIR) program that is aligned to ISO 30111:2013(E) and ISO 29147:2014(E) and is a member in good standing of the Forum for Incident Response and Security Teams (FIRST).

6.2.0 Product development requirements

The product security policies define the following product development requirements for all new, internally developed products:

- Must conform to the Johnson Controls baseline product security requirements and coding practices
- Must assign cybersecurity resources to each product development project to assure products are securely developed in compliance with policies
- Must have software designs modeled according to the Johnson Controls threat modeling standards
- Must have all open source code used in products analyzed and scanned for known vulnerabilities and deprecated code
- Must protect Johnson Controls source code against unauthorized access
- Must make available installation instructions on how to securely install and configure the product and harden it against compromise
- Must maintain Johnson Controls policy compliance records
- Must have compliance records reviewed by a lead security champion and approved before software is released

6.3.0 Security training - Product development

Advanced security training is integrated into the Johnson Controls Product Security Program and requires all application developers have completed the designated developer specific cybersecurity training curriculum for their role.

Ongoing instructor-led training (ILT) and computer-based training (CBT) courses are provided to developers for cybersecurity practices, application security and secure software development topics. The developer training program consists of both mandatory and recommended courses.

6.4.0 Baseline product security requirements and coding practices

Security baseline requirements derived from established cybersecurity standards (e.g. OWASP, NIST SP 800-53r5, ISA/IEC 62443, UFC 4-010-06), tailored for operational technology domain and address 14 core threat categories, including:

- Authentication
- Access control
- Session management
- Data protection
- Malicious input handling

In addition to baseline requirements, our Security Architects work with project teams and their Security Champions to determine the appropriate safeguards each solution must include based on their application, deployment environment and applicable standards and regulations.

6.5.0 Product security testing practices

A variety of in-house or external security testing are conducted as appropriate for the product's target feature set and application, which may include:

- Peer code reviews conducted throughout development
- Source code assessments
- Vulnerability scans
- Fuzz testing
- Penetration testing

Third-party assessments, including penetration tests, are conducted as required. Security architects and development teams use multiple tools and strategies to reduce risk, including:

- Unit test frameworks
- Continuous Integration/Continuous Deployment (CI/CD)
- Static Application Security Testing (SAST)
- Open source code scans

6.6.0 Supply chain management practices

Johnson Controls validates third-party suppliers of critical products, components and technology against our product security and secure development requirements.

6.7.0 Security integration

Our integrated toolchain provides efficient and effective safety measures for achieving and maintaining product security. Security integration is applied to:

- Managing requirements
- Secure code development processes
- Supply chain management
- Compliance with standards, regulations, and certifications
- Vulnerability and incident response
- Customer response

As a result of security integration, we can better ensure Johnson Controls is achieving target levels of protection for our solutions. This includes their design and coding, as well as the services we provide around them. This operational efficiency drives alignment with customer requirements, standards and regulations, as well as our own elevated standards.

6.8.0 Security checkpoints

Products go through various stages of development from ideation, requirements gathering, development, testing and deployment. Each phase includes processes for implementing and verifying security measures. No component is promoted to the next phase unless the security considerations are included and approved by the respective owners.

6.9.0 Security roles

Several security roles are formally assigned to support the complex and ever-evolving field of cybersecurity.

Including:

- Security Architect:
  A cybersecurity expert who works with Security Champions to guide them through security requirements, compliance and testing activities. They are also available to answer security questions

- Security Champion:
  A senior product developer or software engineer is chosen for each product within a product team to assist in the compliance process outlined within product security program

- Security Council:
  Security Champions and Security Architects are members of the Johnson Controls Security Council and meet on a regular basis to share challenges and solutions across business units and disciplines

7 Vulnerability management

This section describes our secure product development practices.

7.1.0 Product vulnerability management requirements

The product security policies define the following vulnerability management requirements:

- Vulnerabilities discovered after product is released to market must be addressed as part of the vulnerability management process
- All known vulnerabilities are be classified, tracked and scored
- Product security advisories for critical and high vulnerabilities are posted on the Johnson Controls product security web pages
- Johnson Controls is designated by MITRE as a CNA (Common Vulnerabilities and Exposures (CVE) Numbering Authority) and publishes CVEs for qualifying product vulnerabilities as part of its required process
- Vulnerability disclosures are made in coordination with the Johnson Controls Product Security Incident Response Team (PSIRT)
- Patches and updates for currently supported deployed products are made available to address critical and high vulnerabilities

7.2.0 Vulnerability scoring

Johnson Controls uses Common Vulnerability Scoring System (CVSS) scoring for all internally and externally found security vulnerabilities which could impact our commercially sold products. Johnson Controls policy requires that critical and high vulnerabilities are remediated before the next scheduled release and addressed in currently supported product versions.

7.3.0 Product threat intelligence

Johnson Controls has a Product Threat Intelligence Program that works under our PSIR team and Vulnerability Management Program. Our Product Threat Intelligence Program proactively monitors various open source and paid vulnerability feeds and then submits identified, relevant issues to product development, support and leadership teams. Advisories and product updates are provided as required.

7.4.0 Product Security Advisories

A Product Security Advisory (PSA) communicates an issue that may impact the secure operation of a Johnson Controls product which requires action on the part of the customer or other third party to mitigate an identified threat. These advisories identify the affected products describe the risk and provide mitigation details. An advisory may be released as a result of a vulnerability within the product itself or to communicate the impact of a third-party vulnerability which the product depends on for operation. Mitigations can include configuration changes, or a software patch/update among other guidance.

Sign up to receive communications on vulnerability management releases. Johnson Controls publicly posts all Product Security Advisories on our website at: https://www.johnsoncontrols.com/cyber-solutions/security-advisories

7.5.0 Additional product vulnerability disclosure channels

This section describes additional product vulnerability disclosure channels, including the National Vulnerabilities Database and the United States Department of Homeland Security Industrial Control System.

7.5.1 The National Vulnerabilities Database

Johnson Controls practices responsible vulnerability disclosure as a MITRE CVE Numbering Authority (CNA). As a CNA, Johnson Controls has the ability to self-report 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.

7.5.2 The United States Department of Homeland Security Industrial Control System

We also make notice to the United States Department of Homeland Security Industrial Control System security team. These notices are included when we publish a CVE.

7.6.0 Enterprise vulnerability management

The Johnson Controls vulnerability program is risk-based. Johnson Controls uses third-party threat intelligence services to provide CVSS scoring information. This rating along with the business criticality to Johnson Controls provides the internal scoring of the specific CVE.

The vulnerabilities discovered are stored in a vulnerability repository hub and compared with external threat intelligence for prioritization based on risk. The scored information helps determine the level of criticality in mitigating vulnerabilities. The Patch and Vulnerability Management Policy and associated standard outline the timeframe for mitigation.

8 Incident response

Johnson Controls has procedures in place to prepare for the event of a security incident or breach. Incident reporting can originate with automated tools, through internal discovery, via a service provider, or through notification from an external source. A tiered escalation process is followed that includes initial triage, severity determination and customer notification.

8.1.0 Enterprise security incident response

The Johnson Controls enterprise incident response practices are governed by our Cybersecurity Incident Response Security Governance Standard. Johnson Controls actively monitors and protects against security threats to our enterprise systems using Network Intrusion Detection Systems (NIDS), Network Intrusion Prevention Systems (NIPS), Endpoint Detect and Respond (EDR) and System Information and Event Management (SIEM) tools deployed throughout the organization.

8.2.0 Product security incident response

Johnson Controls maintains a continuous 24/7 incident response service. The Product Security Incident Response Team (PSIRT) is called upon any time a suspected or actual attack has occurred on a deployed and currently supported product. PSIRT also provides prompt intake and response to security researchers, customers or any concerned party who would like to report a product vulnerability or customer security issue involving a Johnson Controls product. PSIRT follows a defined Products Security Incident Response Plan (PSIRP) for product-based incident response.

The Product Security Incident Response Plan is a guideline for practices related to product security incidents, providing direction to PSIRT and product team members when responding to suspected or actual exploitation of vulnerabilities identified for in-scope Johnson Controls products. This includes all confirmed or suspected cyberattacks against products and/or unplanned disclosure of, or actual exploitation of, product vulnerabilities. Using this plan the PSIRT members track vulnerabilities, issues, weaknesses and potential incidents through resolution. Incident response readiness exercises are conducted with regularity to ensure the team and key stakeholders throughout the organization are prepared for product security incidents should they occur.

Product security concerns may be reported as directed on this web page: https://www.johnsoncontrols.com/cyber-solutions/cyber-response.

8.3.0 Product security incident response readiness

Internal employees are trained on our formally documented and approved Product Security Incident Response Plan (PSIRP). For most lines of business an annual exercise is also conducted. This ensures all stakeholders understand their role in responding to reports of product vulnerabilities and/or customer reports of an actual security issue related to one of our products. This program conforms to ISO 30111:2013(E) and ISO 29147:2014 respectively.

8.4.0 Privacy incident response

Privacy incident response is managed by the Global Privacy Office which coordinates with enterprise and product security organizations as required. Once informed, the Global Privacy Office will assist with the investigation, assess the incident under relevant law and provide guidance regarding privacy law and customer contractual agreements, where relevant.

8.5.0 Customer notification

Identified incidents with Johnson Controls products or services impacting the customer's data will be reported to that customer.

9 Enterprise security practices

This section describes our enterprise security practices.

9.1.0 Risk management

The Johnson Controls risk management office manages physical and business-related risk. The Global Information Security organization addresses risks relating to information security. The Johnson Controls Product Cybersecurity group addresses the security of Johnson Controls branded products.

Johnson Controls maintains an evolving registry of organizational assets and maps controls and risk tolerance to these assets for the purpose of mitigating risks as appropriate to business operations, our customers, our employees and global business partners. This risk management program is tied directly into the Johnson Controls insurance and risk transfer programs. Our enterprise risk management function and our audit and assurance partners review and validate risks on an ongoing basis.

Johnson Controls maintains an internal audit department that reports directly to the Board of Directors.

9.2.0 Business continuity and disaster recovery

Johnson Controls has implemented business recovery and business continuity plans. These plans address the enterprise data centers and applications running in third-party locations to ensure Johnson Controls mission critical applications as listed in the company asset inventory system will resume within the established recovery time objectives.

9.3.0 Business continuity

Johnson Controls has a business Continuity Management Program (CMP) which includes resilience strategies, pandemic preparedness, business continuity maintenance, business continuity training, business continuity testing, business impact analysis, employee awareness and preparedness programs, functional recovery plans, crisis communication plans, crisis management plans and CMP testing. The Johnson Controls policy is based on ISO 22301 standard template and is the basis our Business Continuity Plan.

9.4.0 Disaster recovery

Johnson Controls has developed a Disaster Recovery Plan which is derived from the requirements of our Disaster Recovery Policy. Our Disaster Recovery Policy defines requirements for the governance, communication, business impact assessment, planning, execution and staffing associated with the development of recovery plans and procedures designed to protect and recover Johnson Controls information systems and hosted applications in the event of a disaster.

The policy addresses mission-critical applications listed in the company asset inventory system running in enterprise data centers and running in third-party data center locations, and includes SaaS, IaaS, and PaaS applications and services.

9.5.0 Device management

We manage and protect all our devices as part of our security practices.

9.5.1 Computing and mobile device security

End-user computing and mobile devices issued by Johnson Controls are built with and maintain standard configurations and endpoint protection. Laptops are encrypted using industry standard full disk encryption methods to protect stored information from unauthorized access.

9.5.2 Software update and patching

Johnson Controls follows a Vulnerability Management Policy for enterprise system assets, including servers, laptops, computers and mobile devices, which includes the ability to patch or update as applicable.

10 Security memberships

Johnson Controls activity participates in the cybersecurity community and maintains membership within several security organizations, including:

10.1.0 ISA Security Compliance Institute (ISCI)

Johnson Controls is a founding member of the ISA Global Cybersecurity Alliance and voting board member of the ISA Security Compliance Institute (ISCI). ISASecure® is an industry-led initiative established to independently certify the cybersecurity of control systems, automation and internet of things (IoT) technology. The ISA/IEC 62443 series of standards is designed to provide a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACS).

For a list of our certifications visit our Cyber Solutions website at https://www.johnsoncontrols.com/cyber-solutions.

10.2.0 ISAGCA

Founding member. International Society of Automation's Global Cybersecurity Alliance (GCA).

10.3.0 FIRST

Full member. Forum of Incident Response and Security Teams (FIRST).

10.4.0 MITRE

Common Vulnerabilities and Exposures (CVE®) Numbering authority.

11 Audit, security standards and compliance

This section describes our audit, security standard, and compliance practices.

Johnson Controls maintain robust compliance programs, including regular internal audits of its processes. Audits and certifications vary by product line and product.

11.2.0 ISASecure Secure Development Lifecycle Assurance Certification (SDLA)

The Johnson Controls Global Secure Product Development Process is ISASecure Secure Development Lifecycle Assurance (SDLA) certified globally by the International Society of Automation (ISA)'s ISASecure program. This ISASecure SDLA certification provides customers with assurance that Johnson Controls building technologies and solutions are developed in accordance with the internationally recognized ISA/IEC 62443-4-1 cybersecurity standard.

The ISASecure program was established to independently certify the cybersecurity of operational technology and automation control systems, such as those deployed within smart buildings. SDLA certification specifies security process requirements and practices for the secure development, maintenance and support of these technologies. Johnson Controls received the SDLA conformance certificate from exida LLC, an ISASecure and ISO 17065 accredited certification body, as a result of assessing product development practices used at engineering centers throughout the world.

11.2.1 Cyber essentials (United Kingdom)

Johnson Controls maintains Cyber Essentials (Certificate Number: 7197395) and Cyber Essentials PLUS (Certificate: p-7197395) under our subsidiary company, Tyco Fire and Integrated Solutions UK Limited, operating in the UK.

12 Summary

These security practices, combined with the Johnson Controls cybersecurity organizational structures and policies, enables Johnson Controls to address product security holistically throughout the lifecycle of each product.

Visit the Johnson Controls Cyber Solutions page to learn more about our approach to cybersecurity.

https://www.johnsoncontrols.com/cyber-solutions/

About Johnson Controls

At Johnson Controls (NYSE:JCI), we transform the environments where people live, work, learn and play. As the global leader in smart, healthy and sustainable buildings, our mission is to reimagine the performance of buildings to serve people, places and the planet.

Building on a proud history of more than 135 years of innovation, we deliver the blueprint of the future for industries such as healthcare, schools, data centers, airports, stadiums, manufacturing and beyond through OpenBlue, our comprehensive digital offering.

wtfolio of building technology and software as well as service solutions from some of the most trusted names in the industry.

Visit **www.johnsoncontrols.com** for more information and follow @johnsoncontrols on social platforms.