Rockwell Automation Data Handling Commitments: Information Security, Privacy, and Architecture

Rockwell Automation's Commitment to Responsible Data Handling

Rockwell Automation's information security and privacy programs are based on a holistic strategy, designed to ensure the security and appropriate handling of all data, commercial or personal, by Rockwell Automation or in its Connected Enterprise Ecosystem.

We seek to align our cybersecurity practices to industry-leading standards and frameworks, to enable the enterprise to identify, protect, detect, respond, and recover from security incidents. We also use secure, certified product and service lifecycles in our development and delivery of products.

Our privacy-program is benchmarked to the General Data Protection Regulation ("GDPR"). Rockwell Automation is committed to not only meeting GDPR compliance globally but imposing additional safeguards where necessary in specific jurisdictions.

Purpose: Minimum-Security Commitment, Technical and Organizational Measures

Rockwell Automation is a large organization serving many customers, oftentimes in multi-tenant SaaS environments or using its established enterprise-wide controls. This wide and diverse scope makes it impossible for Rockwell Automation to agree to varying security and privacy requests from multiple customers. Therefore, the purpose of this document is to provide an overview of the technical, physical, and administrative controls that Rockwell Automation uses to protect its products, services, solutions, and IT and OT environments, including the data traversing them.

Minimum Security Commitment

For customers seeking confirmation that Rockwell Automation employs appropriate controls to protect the customers' information, this document provides information that will allow them to assess Rockwell Automation's controls; essentially, these are the minimum standards that Rockwell Automation can agree to follow. In most (if not all) instances, we believe the controls we have adopted are commensurate to or more protective than prevailing industry-standards, meaning that customers needing to "flow-down" security requirements should typically be able to rely on this statement, which has been incorporated by reference into all our standard agreements.

TOMs

GDPR Article 32 requires controllers and processors to implement "appropriate technical and organizational measures to ensure a level of security commensurate to the risk" to personal data. Thus, where Rockwell Automation is handling personal data—particularly when it is acting as a processor on behalf of its controller customers—we will make Rockwell Automation's statement of

its Technical and Organizational Measures, also called its "TOMs," available on our Trust Center at https://www.rockwellautomation.com/en-us/trust-center.html.

Scope

This document applies to the following Rockwell Automation offerings:

- Rockwell Automation IT infrastructure, generally, to the extent that Rockwell Automation is handling personal information or customer data
- MyRockwell
- Rockwell Automation's SaaS offerings within FTHub
- Plex
- Fiix

Note that some of the foregoing offerings may offer controls, certifications, or other protections that exceed what is specified in this document. In no event will these differentiated offerings provide a lower level of security than what is specified in this document.

To the extent that a customer uses "on-prem" Rockwell Automation offerings, such that data is being hosted, stored, transferred, or otherwise handled by a customer or its designee(s), this document will apply only to that portion of offerings actually provided by Rockwell Automation. For example, where a customer is hosting their own data, Rockwell Automation is not responsible for protecting the customer's data using the minimum-security standards described herein.

Frameworks, Organizational Structure, and Personnel

Cybersecurity

The cornerstone of Rockwell Automation's cybersecurity program is the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The NIST CSF is a risk-based approach aimed at managing cybersecurity risks. While no company is 100% immune from cybersecurity breaches, incidents, or attacks, Rockwell Automation seeks to align its practices to the NIST CSF to best mitigate the risks that threaten Rockwell Automation and its customers. Rockwell Automation has applied the NIST CSF in the following areas of its business:

- Enterprise Functional Operations
- Manufacturing Operations
- Product and Services Development

The NIST CSF is dynamic in nature, allowing Rockwell Automation to internally and externally assess its level of maturity related to cybersecurity controls on a regularly reoccurring basis to continuously adapt to changing technologies, threats, and capabilities.

Rockwell Automation manages cybersecurity risk as part of our overall Enterprise Risk Management program. Our strategy was developed and is being executed by security leaders from across the company, including our Chief Information Officer, Chief Information Security Officer, Chief Product Security Officer, VP General Manager Customer Support and Maintenance, and VP General Manager

Systems and Solutions Business, with support from our business leaders and liaisons within each business unit and function, and with oversight by the board of directors. These organizations work together in alignment to the NIST CSF to ensure Rockwell Automation operates with a security focus on its enterprise operations as well as its development of products, applications, and services. Rockwell Automation has also established an Executive Security Council (ESC) composed of members of Rockwell Automation's senior level management who provide additional oversight to the security strategy program.

Privacy

Europe's GDPR is the benchmark for Rockwell Automation's privacy program. Rockwell Automation seeks to align its global privacy practices to the GDPR, with individual jurisdictions subject to heightened requirements where appropriate.

Rockwell Automation has a Chief Privacy Officer and a Privacy Office, consisting of supporting team members, who together administer the privacy program, including maintaining program materials, responding to data subject requests, and responding to privacy incidents. Privacy inquiries can be directed to privacy@ra.rockwell.com.

Rockwell Automation handles non-employee/-contractor personal data consistent with its Privacy and Cookies Policy, together with applicable terms in the Agreement, DPA, or other governing documents.

AI Governance

Rockwell Automation is committed to responsible AI practices, guided by our core principles of fairness, reliability, transparency, privacy, and security. We manage AI risk as part of our overall Enterprise Risk Management program. Our AI risk mitigation strategy was developed and is being executed by leaders from across the company, including our Chief Information Security Officer, VP AI and Autonomy, and VP Data, Analytics and Insights.

Part of this risk mitigation strategy includes a cross-functional AI governance council that was established to assess the various risks associated with AI usage and development at Rockwell Automation, including privacy, bias and discrimination, confidentiality of Rockwell Automation and customer information, security, safety, and third-party intellectual property rights. The council maintains an inventory of AI use, categorizes the AI use by risk level, and promotes compliance with existing and future AI laws and regulations, such as the European (EU) AI Act. AI usage that is deemed to be prohibited AI, as defined under the EU AI Act, such as AI systems that provide social scoring, are not permitted for use at Rockwell Automation.

Many Rockwell Automation products incorporate traditional AI and machine learning functionality, but some Rockwell Automation products and services implement generative AI functionalities, such as FactoryTalk® Design StudioTM Copilot, FactoryTalk® Analytics™ VisionAI™, Fiix® Foresight and Asset Risk Predictor, and Kalypso® (services). Usage of your data in an AI model is dependent on the specific product offering and is governed by the legal terms and conditions outlined in the agreements pertaining to your use of Rockwell Automation products and services, such as our Software and Cloud Services Agreement, DPA, and any other Terms of Use that accompany the in-scope offering.

Statement of Controls

The following describes the technical, administrative, and physical controls employed by Rockwell Automation in connection with the in-scope offerings. These constitute the "minimum-security" standards that Rockwell Automation agrees to employ as part of its contractual relationship with customers. These terms also describe the TOMs used to safeguard personal data; unless stated otherwise, the same controls apply to personal data (*i.e.* are part of Rockwell Automation's TOMs) as to other data handled as part of the in-scope offerings. In the event of any conflict in terms between this Statement of Controls (the "Statement") and the Agreement, the terms of this Statement shall prevail.

Terms and Definitions

The following definitions shall apply for purposes of this Statement. Capitalized terms not otherwise defined in this Statement shall have the meaning set forth in the Agreement. If not defined in the Statement or the Agreement, the term shall be given its commonly understood meaning.

"**Affiliates**" means a person or entity directly or indirectly controlling, controlled by, or under common control of a Party.

"**Agreement**" means the written services or supply agreement between Customer, or any of its Affiliates, and Rockwell Automation.

"**Information Security Incident**" means the confirmed unauthorized or unlawful acquisition, access, processing, destruction, loss, alteration, damage to, use, or disclosure of Customer Information.

"**Customer**" means the Party on behalf of whom Rockwell Automation is providing Services.

"**Customer Information**" means all Customer information and data shared with or provided to Rockwell Automation by Customer or at Customer's direction as part of the Services.

"**Rockwell Automation**" means the Party acting as primary provider of Services and any of its Affiliates that assists in the providing of Services.

"**Service**" or "**Services**" means the service(s) to be provided by Rockwell Automation under the Agreement, including SaaS and cloud-computing services; cybersecurity and networking services; and engineering, installation, and product-support services.

"**Subcontractor**" means an entity who is contractually engaged and authorized by Rockwell Automation to assist in providing Services in connection with the Agreement on behalf of Rockwell Automation.

Minimum Controls

Rockwell Automation implements and maintains commercially reasonable administrative, technical, and physical safeguards designed to protect the confidentiality, integrity, and availability of Customer Information and to avoid the accidental, unlawful, and unauthorized access, use,

destruction, loss, theft, disclosure, corruption, or alteration of Customer Information in the possession of, under the control of, or being processed by Rockwell Automation or Subcontractors. Customer Information is used as reasonably necessary for performing Services under the Agreement, or as directed by Customer. Consistent with the foregoing, Rockwell Automation does the following:

1. ***Security Governance.*** Rockwell Automation appoints a Chief Information Security Officer (CISO) within its own organization responsible for overseeing and enforcing information security policies. Rockwell Automation maintains, reviews, and updates its formal information security program along with a set of information security policies that align to an industry acceptable security governance framework such as ISO 27001, SOC 2, or NIST CSF. Rockwell Automation takes commercially reasonable steps to update this information security governance program, security controls, and policies as needed to continue to align with commercially reasonable changes in industry security standards for as long as Rockwell Automation maintains Customer Information.

2. ***Security Awareness.*** Rockwell Automation maintains its information security awareness program for its employees and Subcontractors and, on at least an annual basis, deploys mandatory security awareness training that makes recipients aware of their responsibilities with regards to information security and the handling of commercial information. Rockwell Automation requires all necessary employees and Subcontractors to complete the mandatory security awareness training.

3. ***Risk Assessment.*** Rockwell Automation conducts a self-assessment of information security risk on at least an annual basis. Rockwell Automation manages risks to Customer Information and Rockwell Automation systems supporting the Services in accordance with a structured risk management methodology or documented risk management procedure. Rockwell Automation seeks to promptly remediate any identified risks impacting Customer Information or assets used to store or process Customer Information.

4. ***Human Resources Security.*** Rockwell Automation ensures that the Services performed hereunder by Rockwell Automation, its employees, agents, and Subcontractors, will be performed by persons who are under confidentiality agreements and trained to provide the Services in a competent, professional, and ethical manner. Background checks, consisting of professional and criminal at minimum, are completed where feasible, appropriate, and permitted by law.

5. ***Physical and Environmental Security.*** Rockwell Automation uses appropriate security controls (e.g., alarms, cameras, locks, badge readers, etc.) designed to protect Rockwell Automation's facilities, areas, rooms, and IT equipment from unauthorized physical access and environmental threats (e.g., fire, flood, temperature change, etc.).

6. ***Logical Security.*** Rockwell Automation utilizes appropriate security controls designed to protect Rockwell Automation's IT equipment, systems, applications, databases, and all electronically stored information from unauthorized access. This includes, but is not limited to, the commercially reasonable use of authentication, access controls, and encryption of Customer Information at rest and in transit.

7. ***Identity and Access Management.*** Rockwell Automation implements and maintains an identity and access management program with procedures that provide industry standard user administration, identification, authentication, and authorization mechanisms. Rockwell Automation supplies the minimum level of privilege and access to individuals, as necessary to allow such individuals to perform an authorized function or role, as such necessity is determined by Rockwell Automation in its sole discretion. User accounts assigned to an individual are not shared. Passwords following industry standard practices are enforced on all accounts to prevent unauthorized access. Based on risk, user accounts and their corresponding privileges are reviewed by Rockwell Automation authorized personnel to verify or modify privileges based on currently assigned function or role. Rockwell Automation revokes all access from voluntarily and involuntarily terminated employees and Subcontractors and revokes all Customer Information access from Rockwell Automation personnel when Rockwell Automation determines that access by such personnel is no longer required for providing Services.

8. ***Change Management.*** Rockwell Automation implements and maintains a change management process designed to ensure that only authorized individuals are planning, documenting, testing, approving, communicating, implementing, and reviewing post-change outcomes, potential rollbacks, and security implications of all process, procedure, hardware, and software changes applicable to the Services.

9. ***Asset Management.*** Rockwell Automation implements systems, end-user devices, and applications, collectively named "computing assets", using standardized builds whenever technically feasible that include a secured, hardened baseline, including known vulnerability patches reasonably applied and malware protection software installed and configured to receive regular updates. Rockwell Automation maintains computing assets with appropriate vendor patches and complete routine maintenance in a reasonably timely manner following established change management procedures.

10. ***System Monitoring and Vulnerability Management.*** Rockwell Automation performs monitoring, patching, security log collecting, and intrusion detection activity for its systems in a commercially reasonable manner, looking for Information Security Incidents, system vulnerabilities, and suspicious external or internal activity. Rockwell Automation seeks to remediate, without undue delay and based upon risk level, identified vulnerabilities or activity that directly impacts Customer Information, assets used to store or process Customer Information, or Services provided to Customer.

11. ***Network Security.*** Rockwell Automation designs, implements, and maintains physical and wireless networks to be resilient, with industry standard security controls designed to prevent unauthorized access and protect network integrity. Network security controls include, but are not limited to, hardened firewalls, routers, switches with content and packet filtering, IDS/IPS, segmentation, and event logging/monitoring. Information system asset controls include, but are not limited to, hardened operating systems, industry standard anti-virus/anti-malware, host-based firewall, and full disk encryption. Event logging from network and information system devices is monitored by authorized security personnel. Where Rockwell Automation personnel uses Rockwell Automation workstations/laptops, Rockwell

Automation is responsible for applying standard technical and organizational security controls. Where Rockwell Automation personnel use workstations from the Customer or accesses the customer network, system or infrastructure, Customer is responsible for applying Customer's standard technical and organizational security controls.

12. ***Incident Management.*** Rockwell Automation implements and maintains threat detection systems and an incident management process that includes the identification, response, recovery, and post-recovery root-cause review for all Information Security Incidents while taking commercially reasonable actions to minimize the incident from reoccurring. The incident management process is documented and tested on at least an annual basis.

13. ***Business Continuity and Recovery Planning.*** If Rockwell Automation is responsible for the control of Customer Information in the scope of the Agreement, Rockwell Automation shall provide commercially reasonable access to such Customer Information during incidents, disruptions, or disasters, as feasible and in alignment with terms of the Agreement and an applicable Service Level Agreement. Such plans are tested on at least an annual basis.

14. ***Subcontracting of Services.*** Services, or parts thereof, may be subcontracted by Rockwell Automation to a Subcontractor or Subcontractors. Selection of Subcontractors are made in Rockwell Automation's sole discretion. Subject to the limitation of liability in the Agreement, Rockwell Automation remains liable for acts of its Subcontractors performed in connection with the Services. Rockwell Automation requires that its Subcontractors agree to security provisions no less stringent than the requirements of this Statement and all applicable laws. Not more than once per year, Customer may request from Rockwell Automation a list of Subcontractors performing Services under the Agreement, and Rockwell Automation shall provide such list within a reasonable time.

15. ***System and Software Development.*** Rockwell Automation follows a defined and secure software development lifecycle process. Authorized and role-trained employees are utilized to develop and maintain software. Secure coding, testing, and maintenance industry standard practices include, but are not limited to, logged check in/check out of source code, version control, static/dynamic code analysis, code audits/reviews, vulnerability release management, and penetration testing when applicable. Rockwell Automation's development processes and procedures are in alignment with industry accepted practices (e.g. OWASP, IEC 62443).

16. ***Information Retention, Return, and Destruction.***

    A. Upon Customer written request and after termination of the Agreement for any reason or expiry of its term, Rockwell Automation securely deletes, or if promptly directed in writing by Customer, returns and does not retain Customer Information related to this Agreement in its possession or control. The obligation to return or destroy all copies of Confidential Information does not extend to automatically generated back-up copies which are not readily accessible provided that Rockwell Automation makes no further use of those copies, and such copies are treated as confidential and are deleted pursuant to an overwrite/retention schedule.

B. Notwithstanding the preceding paragraph, Rockwell Automation is entitled to retain copies of Customer Information to the extent required by applicable law, by regulation, or at the direction of a government/regulatory body but remains subject to all confidentiality terms in the Agreement and requirements within this Statement until destruction, return, or encryption is completed following commercially reasonable records retention governance.

17. ***Information Security Incident Response.*** If Rockwell Automation or a Subcontractor discovers, detects, or is notified of any Information Security Incident that has impacted Customer Information, Rockwell Automation will:

    A. Without undue delay after validating an Information Security Incident, notify Customer in writing of the Information Security Incident. The written notice will, at minimum contain the following information to the extent known to Rockwell Automation at the time of the notification: (i) the date and time of the Information Security Incident; (ii) a description of the nature of the incident; (iii) known details of the Customer Information involved in the Information Security Incident, including, as applicable, the categories of Customer Information and the number of Customer Information records; (iv) a description of the likely consequences of the Information Security Incident on Customer Information; and (v) the steps Rockwell Automation has taken to investigate, contain, and mitigate the Information Security Incident. Rockwell Automation will continue to provide updates of this information to Customer until Rockwell Automation determines the Information Security Incident is resolved.

    B. Conduct a forensic investigation, if or as required by law taking caution to preserve evidence. Rockwell Automation will then seek to remediate issues identified in the forensic investigation as causing the Information Security Incident. Subject to the documentation and audit rights identified elsewhere in this Statement and to the written notification described in the preceding paragraph, Customer acknowledges that it has no right to receive original versions or copies of documents prepared by Rockwell Automation as part of its efforts to comply with this Section, including forensic investigation reports, identification of root causes, or documentation of actions taken to address the issues identified in the forensic investigation as causing the Information Security Incident or to prevent the same or similar risks from recurrence.

    C. Reimburse Customer for reasonable and necessary expenses incurred by Customer in responding to and as a direct result of an Information Security Incident, if the Information Security Incident resulted from Rockwell Automation's noncompliance with its obligations under this Statement. Any such reimbursement shall be subject to the limitations of liability within the Agreement.