Honeywell Security Terms and Conditions

for Third Parties

Prepared by: Honeywell Global Security

Version: 1.0

Effective Date: August 3, 2026

Table of Contents

Honeywell Supplier Security Requirements

1. Purpose & Scope

This document defines the requirements that apply to all suppliers providing products, software, services, or deliverables to Honeywell, and/or those working with confidential information from Honeywell or its customers ("Customer Confidential Information"). These requirements establish the minimum cybersecurity standards that suppliers must maintain throughout the lifecycle of their engagement with Honeywell.

Applicability

Requirements are organized into 13 sections covering organizational security, physical security, network and communications, security operations, and product security (including Artificial Intelligence (AI)/ML and Commercial Off-The-Shelf (COTS)). Not all sections apply to every engagement. The Applicability Matrix following the Table of Contents identifies which sections apply based on the type of product or service being procured. Where a Supplier engagement spans multiple service types, all sections applicable to any of the relevant service types shall apply. The most stringent requirement shall govern where overlapping requirements specify different thresholds. If there are any questions regarding applicable service type for your engagement, please contact CPSS@honeywell.com.

Exception Handling

If any of these requirements cannot be met, the supplier shall promptly notify their Honeywell focal. Any exceptions must be approved by a Honeywell representative and will be for a limited duration of no more than 365 days.

Compliance Program

As a condition of engagement, Supplier shall develop, implement, and maintain a compliance program to ensure organizational compliance with the controls set forth in this document. Supplier shall identify relevant legislative, statutory, regulatory, and contractual requirements and document compliance procedures. Supplier shall monitor these requirements for changes and update the compliance program accordingly. Suppliers shall monitor and audit controls at least once annually to ensure effective implementation.

Standards Attestation

Where this document refers to international cybersecurity standards in lieu of detailed control requirements, Supplier shall attest to adherence with the referenced standards and provide evidence of compliance upon request, including but not limited to certifications, audit reports, or third-party attestations. Suppliers that cannot attest to the referenced standards nor comply with the controls set forth in this document will need to let Honeywell know such that the security exhibit negotiation can be commenced.

Modifications

These security terms and conditions may be modified from time to time to reflect changes in the threat landscape, regulatory requirements, or Honeywell security standards. Suppliers will be notified of material changes and is expected to maintain compliance with the most current version.

Risk-Based Applicability

The requirements set forth in this document are applied on a risk-based basis, with the scope and depth of applicable controls determined by the nature of the products, services, data, and systems involved in the engagement. The applicability matrix designates which sections apply to each service type.

Referenced Standards

These requirements are aligned with the following international cybersecurity standards and frameworks:

- International Electrotechnical Commission (**IEC**) **62443** (Industrial Automation and Control Systems Security) - Parts 3-3, 4-1, 4-2
- National Institute of Standards and Technology (**NIST**) **SP 800-53 Rev. 5** (Security and Privacy Controls)
- **NIST SP 800-218** (Secure Software Development Framework)
- International Organization for Standardization (**ISO**)**/IEC 27001:2022** (Information Security Management Systems)

2. Security Control Applicability Matrix

Service Type	Applicable Control Families												
	Acceptable Use	Incident Mgmt	Info Protection	Logical Access	Minimum Security	Network Security	Personnel Security	Physical Security	Product Dev	Remote Access	Shipping	Supplier Audit	Supplier Facility
Cloud Service – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS)		X	X	X		X	X		X			X	X
Co-lo – No Access to HON Data		X				X	X					X	X
Consultant / Sales Representative *					X								
Data Transport		X	X										
External IP – No Hosting		X	X	X		X	X					X	X
Manufacturing – Hardware Only		X	X	X		X	X				X	X	X
Manufacturing – Hardware & Software		X	X	X		X	X		X		X	X	X
Manufacturing – Low Risk *					X						X		
On Site Access – With Network Access	X	X					X	X					
On Site Access – Without Network Access		X					X	X					
Product Development – COTS		X		X		X	X		X			X	X
Product Development – Custom		X	X	X		X	X		X			X	X
Remote Network Access	X	X								X			
Shipping Only		X					X	X			X		
Transportation / Lodging *					X								
Warehouse Management – Supplier Facility		X	X									X	X

* Minimum Security applies as a baseline for low-risk engagements where no Highly Confidential or Restricted Information is in scope. Product Development includes AI/ML and COTS subsections as applicable. Where a Supplier engagement spans multiple service types, all sections applicable to any of the relevant service types shall apply.

3. Acceptable Use of Honeywell Information

Applicability: This section applies when Supplier personnel are granted access to Honeywell information resources, including systems, networks, or applications, whether on-site or remote.

Section	Security Requirements Detail
Information Resources	**3.1.1** Honeywell Information Resources, including information stored on or transmitted through them, are the sole property of Honeywell and are issued primarily for business purposes and shall be used in accordance with this security exhibit. **3.1.2** Honeywell has no obligation to store, retain or protect any non-Honeywell information. Honeywell may at any time delete any non-Honeywell information on Honeywell Information Resources without advanced notice or further obligation. **3.1.3** Supplier shall have no expectation of privacy on its usage of Honeywell's Information Resources, or the information stored on, or transmitted through them. **3.1.4** Use Customer Confidential Information in a manner consistent with this security exhibit. **3.1.5** Exercise due care in safeguarding Customer Confidential Information Resources provided against loss or damage until they are properly returned. **3.1.5.1** Do not share Customer Confidential Information with unauthorized parties. **3.1.6** Refrain from: • Attempting unauthorized access or resource tampering or misrepresentation. • Interfering with or disrupting the work of others, either inside or outside, the Honeywell network. • Installing and/or executing any form of monitoring tool that will intercept data unless this activity is a part of normal job/duty. • Knowingly interfering with the security mechanisms or integrity of Honeywell's information systems. • Circumventing information technology controls or exploiting security vulnerabilities. • Creating, sending, forwarding, replying to, or storing any message that violates the conditions of this exhibit. • Knowingly creating, installing, executing, or distributing computer code, scripts or packages including any malicious code (including, but not limited to, viruses, worms, and spyware) or other destructive programs on any of Honeywell's information systems, regardless of the result.
Electronic Messaging	**3.2.1** Do not conduct Honeywell business with a non-Honeywell e-mail account unless authorized and provided such action does not violate the conditions of this exhibit. **3.2.2** Do not create, send, forward, reply to, or store any message that violates the conditions of this exhibit.
End-User Device Security	**3.3.1** Do not leave workstations, laptops, mobile devices, and other portable devices or terminal unattended without logging out or invoking a password-protected screen saver. **3.3.2** Position all display screens used to handle sensitive or valuable information to prevent unauthorized viewing. **3.3.3** Secure all hardcopy sensitive information and portable storage media when not in use. **3.3.4** Adhere to acceptable use policy section in this security exhibit. **3.3.5** Supplier shall only use company-managed equipment when working with Customer Confidential Information.
Cloud Specific	**3.4.1** Approval must be obtained from Honeywell Global Security prior to signing up for and/or using a cloud service that will process/store/transmit Honeywell information. **3.4.1.1** Access to approved services shall be limited to Honeywell identities (i.e., no personal email accounts or credentials). **3.4.2** Do not agree to any cloud service agreement on behalf of Honeywell; DO NOT click on "I ACCEPT"/"I AGREE" when presented with web page clickthrough agreement items. **3.4.3** Only process/store/transmit Honeywell information in any environment (e.g. "Cloud") in a manner consistent with what is approved. **3.4.4** Do not use cloud services for any purpose other than the intended/contracted purpose as outlined in the Cloud Service Catalog. **3.4.5** Do not use an unauthorized (free or paid) cloud service to process / store / transmit Honeywell Confidential Information. **3.4.6** Do not use your Honeywell credentials or your Honeywell email address when signing up for cloud services that are for personal use (that will not process/store/transmit Honeywell Confidential Information.

Duty to Return Honeywell Assets	**3.5.1** Do not delete any software or Honeywell information from any Honeywell Confidential Information. **3.5.2** Return all Information Resources in good working order along with all documentation, software and configurations. **3.5.3** Return all replaced/refreshed and/or retired Honeywell Confidential Information to Honeywell in a timely manner for proper destruction of reallocation.
Permitted Access to Honeywell	**3.6.1** Permitted access to Honeywell network is restricted to the Honeywell virtual desktop image (VDI) offering or Honeywell-managed equipment for non-Honeywell managed Windows-based equipment. **3.6.2** Permitted access to Honeywell network is restricted to Mac Kickstart offering for Mac-based equipment.

4. Supplier Audit/Assessment

Applicability: This section establishes Honeywell's audit and assessment rights, including self-assessment, independent annual audit, and Honeywell's right to conduct application vulnerability scans and onsite assessments. Applicability to specific engagement types is determined by the applicability matrix.

Section	Security Requirements Detail
Audit and Assessment Planning	**4.1.1** Audit and assessment activities shall be planned and agreed upon in advance by stakeholders in accordance with the requirements below.
Independent Audits and Assessments	**4.2.1** Supplier shall perform control self-assessments on a regular basis and implement plans of action for responding to the findings in a timely manner. **4.2.2** Reviews and assessments shall be performed by an independent party at least annually, or at planned intervals, to ensure the organization is compliant with its contractual obligations including without limitation the terms of this Exhibit, any policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing) or any other obligations Honeywell may have with its own customers or suppliers. The results of such audits will be promptly sent to Honeywell upon request.
Honeywell Right to Audit or Assess	**4.3.1** Honeywell reserves the right to periodically audit the Supplier's environment containing Honeywell's or its third party's information to ensure compliance with its contractual obligations including without limitation the terms of this Exhibit, any policies, procedures, standards and applicable regulatory requirements (i.e., internal/external audits, certifications, vulnerability and penetration testing) or any other obligations Honeywell may have with its own third parties. **4.3.2** The nature of the audit shall be pre-communicated to Supplier and include clarification as to whether Honeywell, or an agreed-upon third party, will conduct the audit. **4.3.3** Where applicable upon Honeywell's sole discretion, physical audits may be conducted onsite with agreed-upon advance notice. **4.3.4** Without notice, Honeywell reserves the right in its sole discretion to conduct application vulnerability scans against Honeywell developed or owned applications hosted within Supplier's managed environment. **4.3.4.1** Any application vulnerability scan or other application assessment activity may be performed upon Honeywell's discretion either by Honeywell or by a third party on behalf of Honeywell **4.3.5** Audits and assessments are designed to be conducted in such a manner where they will not jeopardize any production data of the Supplier. **4.3.6** Following identification of high risk or critical deficiencies as a result of the audit or assessment, Supplier shall submit to Honeywell a remediation plan in a mutually agreeable timeframe with remediation timelines tied to CVSS severity, consistent with the vulnerability management SLAs set forth in Section 12.10.2.2.

5. Incident Management

Applicability: This section applies to all engagement types designated by the applicability matrix. Where notification timelines in this section overlap with product-specific timelines in Section 12 (Product Development), the shorter timeline shall govern.

Section	Security Requirements Detail
Security Incident Management	**5.1.1** Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities. **5.1.2** Supplier shall document the roles, responsibilities and procedures for supplier's incident response and overall incident management program. **5.1.3** Supplier shall establish and maintain an Incident Response Team to ensure timely response to information security incidents. **5.1.4** Supplier shall track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.
Reporting an Incident to Honeywell	**5.2.1** Upon becoming aware of an information security incident involving Honeywell Confidential Information within Supplier custody, notify the Honeywell focal and send a message to the Honeywell Computer Incident Response team at **Security@honeywell.com** within 72 hours. Examples of these incidents include, but are not limited to: • Loss or theft of Honeywell assets or information • Any unauthorized use of, or access to, Honeywell Confidential Information • Passwords or other system access control mechanisms lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed • Disclosure of sensitive Honeywell information to unauthorized third parties **5.2.2** Any unaccounted-for documents that have been classified as Highly Confidential must be treated as a breach in security. **5.2.3** For incidents in Operational Technology (OT) environments, Suppliers shall additionally notify the designated AME site contact within 2 hours due to potential production impact.
EU Cyber Resilience Act (CRA) - Products with Digital Elements	**5.3.1** For products with digital elements subject to the EU Cyber Resilience Act (Regulation (EU) 2024/2847), the Supplier shall report actively exploited vulnerabilities and severe incidents to the relevant Member State CSIRT and ENISA via the Single Reporting Platform using the following timelines: • Early warning: within 24 hours of becoming aware of the actively exploited vulnerability or severe incident • Full notification: within 72 hours of becoming aware, including an initial assessment of severity and impact • Final report for exploited vulnerabilities: within 14 days after a corrective measure is available • Final report for severe incidents: within 1 month after the 72-hour notification submission **5.3.2** Supplier shall test the organizational incident response capability on a periodic basis.

6. Information Protection

Applicability: This section applies when the Supplier handles Honeywell Confidential Information or delivers products or services where information classification, lifecycle protection, breach notification, and supply chain security compliance obligations apply. Subsections covering Defense Federal Acquisition Regulation Supplement (DFARS), Federal Risk and Authorization Management Program (FedRAMP), US Government Cloud, and US Export Compliance apply only when the engagement involves US Government-regulated information (CUI, Covered Defense Information (CDI), Federal Contract Information (FCI)) or cloud services for US Government contracts.

Supplier shall comply with the applicable information protection requirements of **NIST SP 800-53 Rev. 5** or the equivalent controls of **ISO/IEC 27001:2022**. The following supplemental requirements apply.

Section	Security Requirements Detail
Honeywell Asset Protection	**6.1.1** Supplier shall ensure that Honeywell information is protected throughout its lifecycle including creation, use, processing, storage, transmission and destruction within Supplier's control. **6.1.2.** Supplier shall establish and maintain an information classification strategy to identify and properly handle information based on its sensitivity **6.1.3** Supplier shall establish and review on a periodic basis (not to exceed one year) formal policies, standards and procedures to address applicable security requirements. **6.1.4** Supplier shall implement a continuous monitoring strategy to confirm compliance with applicable security policies, standards and other applicable security requirements **6.1.4** Supplier shall ensure the protection of Honeywell information (confidentiality, integrity and availability) in its information systems, networks and supporting information processing facilities in accordance with this security exhibit. **6.1.5 Honeywell Electronic Data Transport** Supplier shall maintain the confidentiality of Honeywell information within its control in accordance with this Master Agreement, unless otherwise required by applicable law. Supplier must maintain such protection for all data transported through its Services and/or systems, whether transmitted directly by Honeywell or to Honeywell, as part of the Services. Supplier warrants that Supplier will not access nor permit unauthorized persons or entities to access Honeywell computing systems and/or information without Honeywell's express written authorization and any such actual or attempted access must be in accordance to prior authorization. Supplier must immediately notify Honeywell of a potential security breach of these Services or systems, an impending work stoppage, strike, or other interference with Supplier's performance of the services. Honeywell may, at its sole discretion, and without incurring any liability to Supplier, terminate such services due to a breach of Honeywell's confidential information. In addition to complying with applicable regulatory requirements, Supplier must adhere to industry standard security practices including, but not limited to: **(i)** ensure that all Supplier personnel with access to Honeywell's confidential information complete security awareness training that includes the protection of such information; and **(ii)** conduct background screening and verification on all employment candidates, contractors and third parties pursuant to local laws, regulations, ethics and contractual constraints.
Risk Management	**6.2.1** Supplier shall establish and maintain a formal risk management program to address probable and/or actual validated internal and external threats that could compromise the confidentiality, integrity, or availability of Customer Confidential Information.
Asset Management - Asset Procurement	**6.3.1** Supplier shall ensure the hardware and software used for Customer Confidential Information maintain currency and have adequate maintenance and warranty coverages.
Asset Inventory	**6.4.1** Supplier shall maintain inventories of its systems supporting Customer Confidential Information throughout their lifecycle (i.e. from procurement to destruction and shall include relevant information in accordance with this exhibit). **6.4.2** Supplier shall establish a mobile device management policy for all mobile devices storing, transmitting or processing Honeywell information that states: • All mobile devices are configurable for remote wipe by the supplier • Honeywell-related information stored on mobile devices must be backed up • Mobile devices must remain compliant with application password policies • Supplier shall employ controls to prevent bypassing built-in security controls on mobile devices

Asset Configuration and Control	**6.5.1** Supplier shall monitor and maintain the configuration settings of all computing systems used for Customer Confidential Information. **6.5.2** Supplier is responsible for protecting Honeywell`s Confidential Information, from damage, theft, misuse, or unauthorized use.
Asset Removal	**6.6.1** Supplier shall ensure that no Customer Confidential Information remains on assets to be removed from its facilities.
Return of Systems Working with Confidential Information	**6.7.1** Supplier shall implement and maintain a return of information assets policy and procedures to include the return of its systems working with Honeywell assets within supplier's control.
System Disposal for Confidential Information	**6.8.1** Suppliers shall destroy, return, or retain in a compliant manner all Honeywell resources in their possession and comply with any additional requirements upon agreement completion/termination/expiration in accordance with regulatory requirements. **6.8.2** Where such assets are no longer needed, and where the determination is to dispose of such asset, Supplier shall securely dispose of those assets consistent with industry disposal standards and proportional to the security classification of the information or in accordance to what has been agreed-upon with Honeywell. **6.8.3** Suppliers shall maintain a log of all Honeywell physical information assets that have been either disposed of or prepared for reuse following sanitization.
Encryption Management - Use of Encryption	**6.9.1** Encrypt Honeywell Highly Confidential or sensitive information at rest at all times, no matter where located, in accordance with this exhibit. (i.e. information residing in databases, applications and mobile or storage devices). 6.9.1 .1 Transparent Data Encryption (TDE) to be in place for structured data and file or folder encryption for unstructured data. **6.9.2** Supplier shall monitor, control, and protect communications (i.e., information transmitted or received by organizational systems) at the external boundaries and key internal boundaries of organizational systems. **6.9.2.1** Encrypt nonpublic Honeywell information transmitted over public and/or wireless networks. **6.9.3** Encrypt Honeywell Highly Confidential or sensitive information in transit at all times when within Supplier's environment and control. **6.9.4** All encryption products impacting Customer Confidential Information, regardless of encryption strength, shall always provide Honeywell the ability to access such information. **6.9.5** Use of deprecated or known compromised encryption technologies is prohibited. Transport Layer Security (TLS) 1.3 is required to be supported for all data in transit. If TLS 1.2 must be supported, and not yet globally yet deprecated, disable obsolete cipher suites and enforce modern, strong algorithms (such as ECDHE for key exchange and AES-GCM for encryption). **6.10.** Encryption Key Management **6.10.1.1.** Regarding data encryption at rest for Supplier-managed/owned keys, Supplier shall maintain an industry-standard Cryptographic Key Management System (“CKMS”) to ensure the secure generation, storage, use, distribution, and destruction of encryption keys. The CKMS shall meet or exceed the following minimum requirements: • At least two key custodians must be officially designated. • Split knowledge and establishment of dual control (2 or more persons) shall be employed for cryptographic keys that are used for Root signing services. • Key custodians must ensure that all keys used in a storage encryption solution are secured and managed properly to support the security of the solution. • Key management must be planned to include secure key generation, use, storage and revocation. • Keys shall never be transmitted in clear and always remain in a 'trusted' environment • Key management practices must support the recovery of encrypted data if a key is inadvertently disclosed, destroyed, or becomes unavailable. • Key custodians must ensure that access to encryption keys is properly restricted to approved administrators in accordance with a documented process. • Supplier shall replace known or suspected compromised cryptographic keys immediately and issue new keys. • Private keys must not be stored on the same media and/or virtual instance as the data they protect. • Multi-factor authentication must be required in order to gain access to keys.

	• Keys will be rotated annually and must be replaced before they expire. • Passwords for accessing encryption keys must be complex and hashed with irreversible industry standard algorithms with randomly generated “salt” added to the input string prior to encoding to ensure that the same password text chosen by different users will yield different encodings. • Supplier shall ensure that the cryptographic algorithms are both publicly known and widely accepted and the basis, reasoning, and justification for choosing the key size are documented and demonstrate appropriate understanding of cryptographic algorithms. • Supplier personnel will not access Customer Data except upon documented request or approval from the customer and only to the extent and duration permitted by the Customer.
Encryption Key Strength	**6.10.1** Data in Transit; Advanced Encryption Standard (AES) >= 256. **6.10.2** Data at Rest: AES >= 192 where technically capable. Otherwise, the strongest available, but not less than AES 128.
Certificate Authority	**6.11.1** Supplier will only leverage certificates from an industry standard certificate authority and cannot use self-signed certificates when working with Honeywell information.
Security Operations - Information Asset Security Operations	**6.12.1** Supplier shall follow defined and approved change management procedures for an activity that can affect Honeywell Information Asset/s (e.g. security assessments, audits, hardware and software maintenance, patch management, and contingency plan testing).
Service Providers under the jurisdiction of DFARS	**6.13.1** Suppliers providing operationally critical support, or for which subcontract performance will involve controlled unclassified information (CUI), unclassified controlled technical information (CTI), and/or covered defense information (CDI), shall comply with **DFARS 252.204-7012** Safeguarding Covered Defense Information and Cyber Incident Reporting. Reference: https://www.acq.osd.mil/se/docs/dfars-guide.pdf **6.13.2** Supplier shall protect the confidentiality of backup CUI at storage locations. **6.13.3** Supplier shall enforce safeguarding measures for CUI at alternate work sites. **6.13.4** Supplier shall periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational systems and the associated processing, storage, or transmission of CUI **6.13.5** Suppliers shall control the flow of CUI in accordance with approved authorizations. **6.13.6** Provide privacy and security notices consistent with applicable CUI rules. **6.13.7** Control CUI posted or processed on publicly accessible systems. **6.13.8** Supplier shall protect (i.e., physically control and securely store) system media containing CUI, both paper and digital. **6.13.9** Supplier shall limit access to CUI on system media to authorized users **6.13.10** Supplier shall control access to media containing CUI and maintain accountability for media during transport outside of controlled areas. **6.13.11** Supplier shall achieve and maintain the applicable Cybersecurity Maturity Model Certification (CMMC) level as specified in DFARS 252.204-7021 and 32 CFR Part 170. **6.13.12** The required CMMC level shall be determined by the type of information handled according to 32 CFR Part 170. **6.13.13** Supplier shall notify Honeywell in writing within thirty (30) calendar days of any of the following: • achieving or renewing a CMMC certification at any level; • a material change to Supplier's SPRS score; • expiration, suspension, or revocation of Supplier's CMMC certification; • issuance of a conditional CMMC status (including Plans of Action and Milestones (POA&M) items and the 180-day remediation deadline); or • failure to close out POA&M items within the conditional period, resulting in loss of CMMC status. **6.13.14** Supplier shall maintain current CMMC certification or assessment status as a condition of continued performance under any engagement involving FCI or CUI. A lapse in CMMC status constitutes a material breach of this security exhibit. **6.13.15** Supplier shall flow down the applicable CMMC level requirements to any sub-tier suppliers or subcontractors that will process, store, or transmit FCI or CUI in connection with the engagement. Supplier is responsible for verifying sub-tier compliance before granting access to FCI or CUI. **6.13.16** Where the applicable CMMC level requires a C3PAO or DIBCAC assessment, Supplier shall provide Honeywell, upon request, with (a) a copy of the assessment report or summary letter confirming the certification level achieved, (b) the date of certification and expiration, and (c) evidence that the Supplier's SPRS score is current. Supplier shall make this documentation available within fifteen (15) business days of Honeywell's request.

	6.13.17 The CMMC requirements in this section supplement, and do not replace, the DFARS 252.204-7012 compliance obligations set forth in Section 6.13.1 through 6.13.10 of this exhibit.
Cloud Service Providers under the jurisdiction of FedRAMP	**6.14.1** Cloud services providers, in accordance with **NIST SP 800-145**, storing, processing or transmitting any controlled unclassified information (CUI), unclassified controlled technical information (CTI), and/or covered defense information (CDI), shall meet security requirements equivalent to the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline. Reference: https://www.fedramp.gov/resources/documents/ [**6.14.2** Cloud service providers shall comply with **DFARS 252.204-7012** Safeguarding Covered Defense Information and Cyber Incident Reporting paragraphs C – G (extract printed below). Reference: https://www.acq.osd.mil/se/docs/dfars-guide.pdf **(c) Cyber incident reporting requirement.** **(1)** When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall— **(i)** Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and **(ii)** Rapidly report cyber incidents to Department of Defense (DoD) at http://dibnet.dod.mil. **(2)** Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at http://dibnet.dod.mil. **(3)** Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD- approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see http://iase.disa.mil/pki/eca/Pages/index.aspx **(d) Malicious software.** When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer. **(e)** Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1) **(i)** of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest. **(f) Access to additional information or equipment necessary for forensic analysis.** Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis. **(g)** Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph **(e)** of this clause.
US Government Cloud Requirements	**6.15.1** Any Platform as a Service (PaaS) or Infrastructure as a Service (IaaS) offering must be FedRAMP High certified. **6.15.2** Any Software as a Service (SaaS) product must be FedRAMP Moderate certified. **6.15.3** The environment must be administered by U.S. Citizens in a CONUS location. This applies to all administrators and end users that have access to the sponsor's data or encryption keys. CONUS is defined as the 48 contiguous United States and the District of Columbia. **6.15.4** No dual citizenship is allowed for personnel with access to government data or encryption keys. **6.15.5** All FedRAMP authorized services can be verified at https://marketplace.fedramp.gov/. **6.15.6** Security audit record retention must be extended to 5 years.
US Export Compliance	**6.16.1** Supplier shall not transfer any export-controlled information, technical data, or defense articles to any foreign person, entity, or destination without prior written authorization from the appropriate US Government authority. Export-controlled information includes items regulated under the International Traffic in Arms Regulations (ITAR, 22 Code of Federal Regulations (CFR) 120-130) pursuant to the Arms

	Export Control Act (22 U.S.C. 2778), and the Export Administration Regulations (EAR, 15 CFR 730-774) pursuant to the Export Control Reform Act (50 U.S.C. 4801-4852). **6.16.2** Supplier shall maintain an export compliance program that includes identification and marking of export-controlled information, personnel training on export control obligations, and procedures for screening recipients against applicable restricted party lists. **6.16.3** Supplier acknowledges and agrees that (i) that all data transactions between the Parties are not subject to the U.S. Department of Justice's Final Rule on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern ("Final Rule"); (ii) Supplier will not engage in any subsequent data transactions involving data brokerage of the Government-Related Data or Bulk U.S. Sensitive Personal Data (collectively, "Prohibited Data") with a country of concern or covered person (all terms as defined under the Final Rule); (iii) Supplier will not engage in any subsequent data transactions involving Prohibited Data that would be subject to the Final Rule without Honeywell's prior written permission. Failure to comply with the provisions in this Agreement related to the Final Rule will constitute a breach of this Agreement and may constitute a violation of the Final Rule.
Workstation Security Operations	**6.17.1** Workstation security controls set forth here by Honeywell Security apply to all workstations that access or manage Honeywell information resources. **6.17.2** Supplier shall ensure that all Workstations have an approved operating system image installed. If an approved image is not installed, workstations shall be installed and configured with end-point applications to facilitate centralized administration including malware protection and security patches.
File and Print Sharing	**6.18.1** File sharing is prohibited and shall be disabled on the workstation. Only Administrative File Shares (such as Admin$) are allowed and shall be used by authorized IT personnel. Users shall not share locally attached printers to the network.
Malicious Code	**6.19**. Malicious Code **6.19.1**. Supplier shall employ centrally managed malicious code protection mechanisms to detect and eradicate malicious code at relevant access points. **6.19.2**. Supplier shall, i. Scan its information assets at an industry standard frequency including but not limited to, o When there are changes to the information asset/environment o Persistent scans whereby processes and files are scanned upon read and write access • Where persistent scans (on access) cannot be run, a full disk and memory scan shall be performed at least every 7 days. An exception is required to disable persistent scanning (on access) o Perform full disk and memory scan on workstations at least every 14 days o Perform monthly full disk and memory scan on servers iii. Scan contents of compressed archive files iv. Perform memory scans v. Block and quarantine malicious code vi. Alert designated Supplier teams with applicable malicious code detection information. **6.19.3**. Supplier shall employ a process to automatically update malicious code protection mechanisms whenever new releases are available. **6.19.4**. Supplier shall employ host-based boundary protection mechanisms such as host-based firewalls on Supplier network components (servers, workstations, mobile devices) accessing or managing Customer Confidential Information to help prevent unauthorized access and the spread of malicious software. **6.19.5.** Supplier shall take precautions to ensure that malicious code is not introduced into the Honeywell environment, or to the Supplier environment containing Honeywell information assets. Software shall not be written, generated, copied, propagated or executed that will compromise any Honeywell information asset. **6.19.6**. Suppliers shall ensure operating systems and/or workstation hardware or software have mechanisms to protect memory from unauthorized code execution (i.e. DEP, address space layout randomization, etc.)
Patch Management	**6.20.1** Supplier shall establish and maintain a centralized patch management process to identify, evaluate, report and deploy patches and system updates to any asset working with Honeywell information.
Vulnerability Scanning and Penetration Testing	**6.21.1** Supplier shall identify, report, and correct system flaws in a timely manner. **6.21.1.1** Supplier shall scan its environment for vulnerabilities periodically (on a quarterly basis or more frequently), and when new vulnerabilities affecting the system are identified in accordance with: • Service criticality • Change to the environment • Identification of new vulnerabilities

	6.21.2 Supplier shall conduct periodic external / internal penetration testing on the hardware, software, firmware, and programmable logic components of its assets that access or manage Customer Confidential Information, as defined in the associated procedures **6.21.3** Suppliers shall maintain a security posture of their Internet-facing resources that meets or exceeds the industry average as established through publicly available monitoring solutions.
Configuration Management	**6.22.1** Supplier shall establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, programmable logic, and documentation) throughout the respective system development life cycles for all Supplier assets supporting Honeywell where such are tracked in a sanctioned asset inventory system.
Logging, Monitoring and Reporting	**6.23.1** Supplier shall ensure that internal system clocks maintain synchronization with an accurate universal time source. **6.23.2** Supplier shall retain audit logs for at least 6 months. **6.23.3** Supplier shall log privileged user access, authorized/unauthorized access attempts, system exceptions, and security events. **6.23.4** Supplier shall maintain real-time notification of logging process failures. **6.23.5** Supplier shall maintain automated audit review, analysis, and reporting. **6.23.6** Supplier shall maintain unaltered original logs with timestamps. **6.23.7** Supplier shall protect audit tools from unauthorized access, modification, and deletion. **6.23.8** Supplier shall restrict access to original logs. **6.23.9** Supplier shall integrate audit with incident response processes.
Information Systems Maintenance	**6.24.1** Supplier shall approve and monitor all maintenance activities (performed on/off site or remotely) and explicitly approve the removal of its systems working with Customer Confidential Information from facilities for off-site maintenance in accordance with this security exhibit. **6.24.2** Supplier shall take the following measures to prevent the unauthorized removal of maintenance equipment containing Honeywell information: • Verifying that there is no Honeywell information contained on the equipment • Retaining the equipment within the facility or • Obtaining an exemption from Honeywell management explicitly **6.24.3** Supplier shall check media containing diagnostic and test programs for malicious code before the media are used in organizational systems. **6.24.3.1** Supplier shall screen any software for malicious code before using it for maintenance of its systems working with Customer Confidential Information in accordance with this security exhibit. **6.24.4** Supplier shall employ proper authentication, monitoring and termination mechanisms for nonlocal maintenance and diagnostic activities on its systems working with Customer Confidential Information in accordance with this security exhibit. **6.24.5** Supplier shall supervise the maintenance activities of maintenance personnel without required access authorization.
Compliance - Compliance Program	**6.25.1** Supplier shall develop, implement and maintain a compliance program to ensure organizational compliance with the controls set forth in this security exhibit. **6.25.2** Supplier shall monitor and audit controls at least once annually, to ensure effective implementation.
Risk Management of Suppliers	**6.26.1 Supplier shall establish security requirements with each outsourced supplier and notify the outsourced supplier of such security requirements through specific language appearing in agreements that define their relationship.** **6.26.2** Supplier shall conduct risk reviews of all outsourced suppliers with access to Customer confidential information based on the outsourced supplier Risk Profile at least annually or when there is a change in contract.

7. Logical Access

Applicability: This section applies when the Supplier operates systems or provides personnel with logical access to systems containing Honeywell Confidential Information. It governs user authentication, authorization, account management, and session controls.

Supplier shall comply with the applicable access control requirements of **IEC 62443-3-3** and **IEC 62443-4-2**. The following supplemental requirements apply.

Section	Security Requirements Detail
Access Management	**7.1.1** Supplier shall identify system users, processes acting on behalf of users, and devices. **7.1.1.1** Supplier shall implement a formal access management process to assign, approve, modify and revoke access to Customer Confidential Information and any supporting systems. **7.1.2** Supplier shall assign unique identifiers (username/ID) to all personnel **7.1.3** Supplier shall review access rights granted to privileged accounts on a quarterly basis and update access rights accordingly. **7.1.4** Supplier shall periodically review (not to exceed one year) access rights granted to all other accounts and update access rights accordingly. **7.1.5** Privileged accounts not used for non-security functions **7.1.6** Supplier shall revoke access rights provided to personnel upon employment termination as soon as possible (not to exceed one business day).
Password Management	**7.2.1** Supplier shall maintain the following practices: ○ Support staff password requires a minimum of 10 characters; ○ No username included in password; ○ Change default passwords before production; ○ Verify identity before processing password change requests; ○ Prevent password reuse altogether or enforce password history of 10 or more; ○ Maintain replay-resistant authentication for privileged and non-privileged network access; ○ Configure accounts to be locked out after five (5) consecutive unsuccessful login attempts or similar smart lockout feature to protect against brute-force attacks; ○ Change group/role account passwords on membership change; ○ Obscure password feedback (asterisks); ○ Implement measures to ensure that privileged accounts are not used for non-security functions; ○ Store and transmit passwords in encrypted format only.
Session Control and Timeout	**7.3.1** Supplier shall terminate idle sessions after 15 minutes for any sessions that require authentication or provide access to any non-public resource. **7.3.2** Supplier shall apply screensavers after 15 minutes (except for kiosks intended for shared access) and require the user to authenticate to reestablish access, as technically feasible and consistent with business operations. **7.3.3** Supplier shall grant access to Customer Confidential Information based on the principle of least privilege, allowing only necessary access to accomplish the assigned tasks.
Separation of Duties (SOD)	**7.4.1** Supplier shall establish and maintain procedures to ensure that access, roles and permissions are appropriately segregated to prevent an individual from committing and concealing fraud. **7.4.2** Supplier shall ensure that SOD conflicts are documented and approved in cases where SOD conflicts cannot be avoided. **7.4.3** Supplier shall ensure processes are in place to enforce SOD as follows: • Separate personnel are required for testing, requesting, authorizing and administering access to Customer Confidential Information. • Security personnel administering access control functions are not permitted to administer audit functions.
Privileged Access	**7.5.1** Supplier shall log and audit the actions performed by privileged accounts on Customer Confidential Information.
Identification and Authentication	**7.6.1** Supplier shall not permit any actions to be performed on Customer Confidential Information without successful authentication. The only exception shall be public web servers that allow public access to information intended for public consumption.
Invalid Login Attempts	**7.7.1** Supplier shall lock accounts for thirty (30) minutes or until released by the account administrator.

8. Minimum Security

Applicability: This section establishes minimum physical, technical, and administrative security controls. For engagements designated by the applicability matrix with a limited set of applicable sections, this section provides the baseline security requirements. For engagements with broader applicability, this section supplements the other designated sections with additional baseline expectations. The applicability matrix determines which sections apply to each engagement type.

Section	Security Requirements Detail
Physical Controls	**8.1.1** Control physical access to all facilities and information processing areas with Confidential Information to ensure only authorized persons have access to areas; **8.1.2** Monitor physical access to facilities to detect and respond to physical security incidents; and **8.1.3** Employ appropriate access control mechanisms to control visitors' access to facilities and validate approval of visitors before granting access to facilities.
Technical Controls	**8.2.1** Implement industry-standard technical measures, including a formal access management process in accordance with the principles of "least privilege" and "need to know"; **8.2.2** Configure information management systems to disable/delete inactive personnel accounts after 90 days; **8.2.3** Enforce password complexity requirements with minimum of eight (8) alphanumeric characters of mixed case **8.2.4** Prevent reuse of a password for at least one year; **8.2.5** Configure accounts to be locked out after five (5) consecutive unsuccessful login attempts and terminate idle sessions after fifteen (15) minutes for any sessions; **8.2.6** Employ encryption and strong authentication mechanisms such as hardware token-based authentication or other multifactor authentication (as applicable) for privileged access and remote access; **8.2.7** Encrypt (using industry-standard protocols) Confidential Information and authentication credentials in transit over public and/or wireless networks and when on mobile media or storage devices; **8.2.8** Encrypt all Confidential Information at rest at all times **8.2.9** Maintain whole disk encryption for any mobile devices containing Confidential Information; **8.2.10** Employ protection mechanisms to detect and eradicate malicious code at relevant access points; **8.2.11** Scan environment for vulnerabilities periodically (on a quarterly basis or more frequently) and conduct penetration testing at least annually, and promptly remediate any identified vulnerabilities; **8.2.12** Maintain an enterprise patch management process to identify and deploy patches and system updates to any asset with Confidential Information; **8.2.13** Install security-relevant software and firmware updates in accordance with vendor recommendations; **8.2.14** Monitor the network and key applications, at a minimum, to detect cyber-attacks or indicators of potential attacks or unauthorized or unapproved network services; **8.2.15** Use automated processes and tools, including intrusion detection & prevention, to support real-time analysis of networks; **8.2.16** Maintain an incident response program in compliance with industry standards (e.g., ISO/IEC 30111, ISO/IEC 29147) and notify Honeywell at **Security@Honeywell.com** within 72 hours for incidents involving Honeywell Confidential Information;
Administrative Controls	**8.3.1** Perform, in accordance with applicable laws and regulations, background check screening (including, where not prohibited by law, identity verification and criminal history) on personnel prior to authorizing Confidential Information; **8.3.2** Train all personnel on information security awareness best practices, including insider threat, within 30 days of onboarding or prior to gaining access to Confidential Information, and annually thereafter; **8.3.3** Revoke physical and cyber access rights and mechanisms (e.g. keys or access cards) provided to personnel upon termination as soon as possible (not to exceed one business day); **8.3.4** Upon Honeywell's request, provide sufficient evidence and documentation to demonstrate compliance with Supplier's obligations hereunder

9. Network Security

Applicability: This section applies when the Supplier operates network infrastructure, transmits Honeywell data, connects to Honeywell networks, or delivers products that will operate on networks.

Supplier shall comply with the applicable network security requirements of **NIST SP 800-53 Rev. 5** or the equivalent controls of **ISO/IEC 27001:2022**. The following supplemental requirements apply.

Section	Security Requirements Detail
Network Device and Connection Inventory	**9.1.1** Supplier shall maintain and update on a periodic basis (not to exceed one year), a current inventory of all network devices and relevant documentation on the set up and operation of network devices. **9.1.2** Supplier shall review and update a current network diagram that illustrates all connections that support the Honeywell service at least annually.
Network Design	**9.2.1** Supplier shall employ mechanisms to control the flow of information and implement safeguards and controls as part of its network design to eliminate, protect against or limit the effects of network attacks and unauthorized access to Customer Confidential Information.
Network Configuration	**9.3.1** Supplier shall test and review all firewall configuration rules on a periodic basis (not to exceed one year).
Network Segmentation and Boundary Protection	**9.4**. Network Segmentation and Boundary Protection **9.4.1**. Supplier shall implement boundary protection mechanisms (e.g. proxies, gateways, routers, firewalls) in order to monitor and control communications at the logical or external boundary and at key internal boundaries within the network. **9.4.2.** Supplier shall employ appropriate mechanisms to physically or logically segregate internal networks from untrusted networks such as the Internet. **9.4.3**. Supplier shall configure all boundary protection devices to deny network traffic by default and allow network traffic by exception (i.e., deny all, permit by exception). **9.4.4**. Supplier shall isolate the management of information security tools, mechanisms, and support components from the internal network. This can be achieved through implementing physically separate sub networks dedicated for information security tool management and supporting components. **9.4.5**. Supplier shall employ mechanisms that ensure a secure state in the event of an operational failure of boundary protection devices (e.g. firewalls, routers). **9.4.6.** Supplier shall route all remote access through managed network access control points (to limit access control points for remote access). **9.4.7.** Supplier shall prevent, through configuration, remote connections on any device from establishing multiple connections between dissimilar security domains at the same time (e.g., split tunneling).
Supplier Connectivity to Honeywell	**9.5.1** A site-to-site connection between the Supplier's network and Honeywell internal network must have a firewall. Access to and from Honeywell to the Supplier's network must be reviewed and approved by Honeywell Security. The firewall requirements are as follows: • Use a stateful firewall; Federal Information Processing Standards (FIPS) 140-2; Certified Evaluation Assurance Level 4 (EAL4) compliant • All traffic between the Supplier and Honeywell shall route through the approved firewall. • It is recommended that the Supplier protect its internal network from Honeywell by implementing a Supplier-managed firewall with least access rules. • Rules must specify IP-to-IP access with specific ports and protocols and follow principles of least privileged. **9.5.2** Supplier and Honeywell must each manage their respective network device endpoints. This is desirable for both security and operational reasons. Where applicable, Honeywell requires out-of-band connectivity to the remote endpoint for debugging purposes. **9.5.3** Periodic audits must include external scans of the Internet-reachable devices used to establish the VPN tunnel.
Semi-Trusted Networks - Supplier Security Requirements	**9.6.1** Semi-Trusted requirements apply if a site-to-site connection between Supplier network and Honeywell internal network that requires Least Access firewall rules. Used for outbound-initiated connectivity into the network, or a specific set of inbound IPs/ports/protocols acceptable to Honeywell.
Semi-Trusted Workplace Security	**9.7.1** Restrict physical access to the Supplier's computing resources with access to Honeywell's networks, systems and/or information to only authorized Supplier personnel.

	9.7.2 Maintain visitor logbooks that include visitor's name, purpose of visit, arrival and departure time. A Supplier employee must always escort visitors within the Supplier's restricted area that access or manage Customer Confidential Information.
Semi-Trusted Network Architecture	**9.8.1** Establish firewall filtering rules between the Semi-Trusted Supplier's network and the Honeywell network to limit the access from the Semi-Trusted Supplier's network to only the systems needed to support the business function.
Physical Security Requirements	**9.9.1** Physical Access to Network Demarcation (demarc) Physical access to the network demarcs must be secured and controlled. It can be secured in a dedicated network closet, cage within network closet, locked cabinet, or locked box within a network closet where access is restricted to authorized personnel and dedicated to supporting Honeywell operations. **9.9.2 Change Management for Physical Changes** Any changes to the physical configuration of the Honeywell dedicated enclave must be reported to Honeywell Security.
Logical Security Requirements	**9.10.1 Third Party Network Connections** Network connections from the Honeywell dedicated enclave must not bridge to a third-party network. **9.10.2 Change Management** Any changes to the security posture enforced by the logical configuration of the Honeywell dedicated enclave must be reviewed and approved by Honeywell Security.
Trusted Supplier Networks - Supplier Security Requirements	**9.11.1** Trusted Supplier requirements apply to a physically isolated segment of the Supplier network connected to a Honeywell internal network in a manner identical to that of a Honeywell remote office.
Physical Security Requirements	**9.12.1** Physical Access to Network Demarcation (demarc) Physical access to the network demarcs must be secured and controlled. It can be secured in a Honeywell controlled network closet, cage within network closet, locked cabinet, or locked box within a network closet with restricted access. **9.12.2** Physical Access to the Area Designated for Honeywell Employees and/or Authorized Contractors A workspace must be designated for Honeywell employees and/or authorized contractors. Physical access to this workspace must be secured from floor to ceiling. This area must be dedicated to Honeywell operations. Honeywell controlled access solutions must be implemented with monthly review of access records and a manual visitor log. All visitors must be escorted. **9.12.3 Secure Conduit for any Private Network Wiring** Network wiring must be protected when traversing non-Honeywell-controlled areas. The preferred method is via conduit. **9.12.4 Change Management for Physical Changes** Any changes to the physical configuration of the Honeywell enclave must be reviewed and approved by Honeywell Security.
Logical Security Requirements	**9.13.1 Third Party Network Connections** Network connections from the Honeywell enclave must not bridge to a third-party network. **9.13.2 Change Management** Any changes to the security posture enforced by the logical configuration of the Honeywell enclave must be reviewed and approved by Honeywell Security.
Telecom Security Requirements	**9.14.1** If the facility provides a voice communication network(s) for Honeywell employees and authorized contractors, appropriate standards for securing the voice network must be implemented. Such standards include but are not limited to, secure management of devices, requirements for VoIP, or any other requirements pertaining to voice communication.
Systems and Communications Protection	**9.15.1** Supplier shall employ FIPS-validated cryptography when used to protect the confidentiality of CUI.

10. Personnel Security

Applicability: This section applies to engagements where personnel screening, security awareness training, and employment lifecycle controls are designated by the applicability matrix. For engagements where only Section 8 (Minimum Security) applies, the simplified personnel requirements in that section govern.

Section	Security Requirements Detail
Personnel Screening	**10.1.1** Supplier shall screen, in accordance with relevant laws and regulations, all personnel prior to authorizing access to Customer Confidential Information. **10.1.2** Supplier shall rescreen all personnel upon change in responsibilities which require additional levels of access or authority and in accordance with Government requirements for security screening and clearance. **10.1.3** Personnel Screening requirements include, to the extent permitted by applicable law: • Criminal record checks (criminal history for the previous 7 years) • Social Security Number, National Identifier or Personal Identity Code validation • Validation of citizenship, dual citizenship status, and country of birth **10.1.4** Additional Personnel Screening requirements for Supplier personnel requiring unescorted badge access **to US-based Honeywell Facilities or network access include:** • US persons validation is required when accessing technical information subject to the US export regulations. • Social Security Number, National Identifier or Personal Identity Code validation • National Sex Offender Registry (State Sex Offender Registries are too restrictive) • Drug testing **10.1.5** Additional Personnel Screening requirements apply for Supplier personnel working with US Government-restricted information. US Government restricted information means information the US Government has defined as requiring protection and includes Federal Contract Information (FCI), Controlled Unclassified Information (CUI), and/or export controlled technical data. Accordingly, Supplier will comply with Federal Acquisition Regulation (FAR) 52.222-54 Employment Eligibility Verification, where applicable and Supplier certifies that it is not, nor will it use, a prohibited party on a U.S. or non-U.S. Restricted Party List in support of this [contract, agreement, etc. Restricted Party Lists include, but are not limited to the following: • Exclusions List – Parties debarred or suspended from doing business on US Government federally funded contracts (FAR-based, grant agreements, etc.). This list is stored in System for Award Management (SAM).gov. • Debarred Parties - Parties denied export privileges under the International Traffic in Arms Regulations (ITAR) as administered by the Office of Defense Trade Control (DTC) • Denied Persons List - Parties denied export privileges as administered by the Bureau of Industry and Security. Denial orders are issued by Federal Register Notices and listed on the Bureau of Industry and Security (BIS) website. • Entity List - Entities for which the U.S. Government has determined are involved in activities contrary to national security or foreign policy of the United States. The list may be found in the Export Administration Regulations, 15 CFR Part 744 Supplement No. 4 • Specially Designated Nationals and Blocked Persons, parties subject to Sectoral Sanctions Identifications lists, and parties subject to other economic sanctioned programs administered by the Office of Foreign Assets Control (OFAC). **10.1.6** Supplier shall use a contractor (a 3rd party consultant) to fulfill the personnel screening requirement for criminal history checks and drug testing. **10.1.7** Supplier will maintain an integrity and compliance program effective in preventing and correcting ethical violations and in maintaining compliance with all applicable laws and regulations. Supplier will comply with Honeywell's Supplier Code of Business Conduct, a copy of which may be obtained at http://hwll.co/CodeOfConduct
Information Security Awareness, Education and Training	**10.2.1** Supplier shall implement a formal security awareness program for all personnel with access to Customer Confidential Information that includes providing security awareness training on recognizing and reporting potential indicators of insider threat. **10.2.2** Supplier shall ensure that all personnel complete information security awareness training and testing within 30 days of on-boarding or prior to gaining access to Customer Confidential Information and annually thereafter. Supplier shall test completion to confirm the understanding of the employees (must be sufficiently passed).

	10.2.3 Supplier shall ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.
Personnel Transfers and Changes	**10.3.1** Supplier shall notify appropriate groups in a timely manner when personnel transfer departments or change job functions and modify access rights of personnel accordingly. **10.3.2** Supplier shall communicate security responsibilities and duties following any change in employment status. **10.3.3** Supplier shall ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.
Personnel Employment Terminations	**10.4.1** Supplier shall notify its Human Resources and appropriate groups upon employment termination and ensure the following actions are taken within one (1) business day: • Supplier shall relieve personnel of all their duties. • Supplier shall conduct a review of all accounts (service or privileged) assigned to terminated personnel and access shall be disabled. • Where applicable, supplier shall ensure that terminated personnel return the Customer Confidential Information and information systems assigned to them or in their possession.

11. Physical & Environmental Security

Applicability: This section applies when the Supplier operates its own facilities that house Honeywell information, systems, or physical assets, or handles Honeywell physical goods in transit or storage.

Section	Security Requirements Detail
Honeywell Visitor Management	**11.1.1** All personnel accessing or managing Honeywell assets are responsible for protecting such from damage, theft, misuse, or unauthorized use. In an effort to fulfill this responsibility, only authorized personnel are allowed unescorted access to company facilities. **11.1.2** With proper authorization, photographic identification badges may be issued to Third-Parties, contractors, or others who are assigned to company facilities and report to work there on a daily basis for extended periods. Supplier agrees to collaborate with Honeywell or its designated MSP to generate the Honeywell electronic identifiers (EID/HID), required by Honeywell as part of this process. **11.1.3** Honeywell-provided badges must be worn in a visible manner while the bearer is in any company facility not generally open to the public. **11.1.4** All visitors must be signed in and escorted by a company employee throughout the time that the visitor is in a company facility. **11.1.5** Any Third-Party who discovers an unauthorized individual within a company facility should notify their supervisor or contact site security.
Equipment Inspection & Management	**11.2.1** Any packages, objects, bags, etc. brought into or removed from company facilities are subject to inspection. **11.2.2** Where required by policy and/or site leadership, authorization must precede any equipment, information or software being taken off-site. **11.2.3** Honeywell's security guards may log out and log in equipment as it leaves or enters Honeywell's facility in accordance with established procedures developed by site leadership. **11.2.4** Cameras and single-function recording devices are not permitted on Honeywell premises without prior authorization from site management.
Third-Party Personnel Notification Requirements	**11.3.1** Regularly review and update the access rights of their personnel and when such personnel no longer provide services to Honeywell, notify Honeywell within one (1) business day, except in urgent situations where notification is to be immediate.

12. Product Development

Applicability: This section applies when the Supplier delivers software, firmware, hardware with programmable or configurable logic, or integrated technology products to Honeywell, whether custom-developed, commercial off-the-shelf (COTS), cloud-hosted, or embedded. Subsection applicability varies by product type as defined in the applicability matrix and noted within this section.

Supplier shall comply with the applicable requirements of **IEC 62443-4-1**, **IEC 62443-3-3**, and **IEC 62443-4-2**. The following supplemental requirements apply.

General Product Security

The following requirements apply to custom-developed products and services delivered to Honeywell, including those containing executable code. COTS products are addressed by separate COTS-specific subsections below.

Section	Security Requirements Detail
Evidence of Compliance	**12.1.1** Upon request, Supplier shall provide evidence of cybersecurity compliance through one or more of the following certifications or attestations, as applicable to the product or service being delivered: • EU Cyber Resilience Act (Regulation (EU) 2024/2847) conformity assessment • CE Mark (where applicable to product category) • Third-party security attestations or audit reports • Capability Maturity Model Integration (CMMI) for Development • **IEC 62443-3-3**, **IEC 62443-4-1**, or **IEC 62443-4-2** certification • ISO/IEC 27001 certification • **NIST SP 800-53** compliance assessment or equivalent controls framework
Development Environment Processes	**12.2.1** The Supplier shall have a published risk management policy and a process to enforce and/or execute against that policy inclusive of an exception process. **12.2.1.1** The Supplier shall maintain a risk register to record centrally manage and document mitigation and prioritization of risks. **12.2.2** The Supplier shall maintain inventories of its systems supporting Customer Confidential Information throughout their lifecycle (i.e., from procurement to destruction and shall include relevant information in accordance with this exhibit). **12.2.3** The Supplier shall ensure that Confidential Information related to Honeywell products are sanitized and/or destroyed based on data classification associated with the asset and maintain a log documenting sanitization activity that includes what was sanitized, methods used, and who performed the action.
Development Environment Technical Requirements	**12.3.1** The Supplier shall separate and protect each environment involved in software development. **12.3.1.1** The Supplier's software development environment used to develop, deploy, and support the Products shall have security controls that can detect and prevent any attacks by use of host, application and network layer firewalls and intrusion detection/prevention systems (IDS/IPS). **12.3.2** The Supplier shall store all forms of code - including source code, executable code, and configuration-as-code - based on the principle of least privilege so that only authorized personnel, tools, services, etc. have access. **12.3.2.1** Have the code owner review and approve all changes made to code by others. **12.3.3** The Supplier shall procure industry standard hardware, software, firmware, and programmable logic that is not prohibited by regulatory requirements of the customer's government for use in the development environment. **12.3.4** The Supplier shall log all security relevant events including, as a minimum: • Failed logons • Account lockouts • Logon times • Log tampering and deletion • Failed object access events and High security events over time. These logs shall be retained according to industry and or legal standards set forth for the environment and purpose • not to be less than 90 days
Secure Software Development Lifecycle (**SSDLC**) **Processes**	**12.4.1** A member of the executive team in the organization shall sign-off that the SSDLC was executed appropriately on the product release as attestation that security requirements have been met or exceeded. **12.4.1.1** The Supplier shall ensure all Products have been developed in accordance with principles of secure software development consistent with software development industry best practices such as Open Web Application Security Project (OWASP), Cloud Security Alliance (CSA), IEC62443 and regulatory requirements,

	including, security design review, secure coding practices, risk-based testing, input validation, error detection. Logging/tracing capabilities, and remediation requirements. **12.4.2** The Supplier shall ensure that hardware and software used in the product shall be procured from approved reputable sources. **12.4.2.1** Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks) from commercial, open-source, and other third- party developers for use by the organization's software. **12.4.2.1.1** Obtain provenance information (e.g., Software Bill of Materials (SBOM), source composition analysis, binary software composition analysis) for each software component and analyze that information to better assess the risk that the component may introduce. **12.4.3** The Supplier shall create and maintain well-secured software components in-house following Software Development Lifecycle (SDLC) processes to meet common internal software development needs that cannot be better met by third- party software components. **12.4.3.1** Maintain one or more software repositories for these components.
Secure Code Review	**12.5.1** The Supplier shall ensure that software design and code undergo security review by qualified personnel independent of the development team to verify compliance with all security requirements and address identified risks. **12.5.1.1** Record the findings of design/code reviews to serve as artifacts. **12.5.2** The Supplier shall perform the code review and/or code analysis based on the organization's secure coding standards, and record and triage all discovered issues and recommended remediations in the development team's workflow or issue tracking system. **12.5.2.1** Identify and document the root causes of discovered issues. **12.5.2.2** The Supplier shall document lessons learned from code review and analysis in a searchable knowledge management system accessible to developers.
Data Dictionary	**12.6.1** The Supplier shall provide a document/spreadsheet that contains a list of data elements that are used and stored by the application and includes a classification of those data elements. **12.6.1.1** The Supplier shall use data classification methods to identify and characterize each type of data that the software will interact with.
SSDLC Technical Requirements	**12.7.1** The Supplier shall use compiler interpreter and build tools that offer features to improve executable security. **12.7.1.1** Use up-to-date versions of compiler interpreter and build tools. **12.7.2** The Supplier shall ensure the hardware and software used in Honeywell product maintain currency and have adequate maintenance and warranty coverages. **12.7.3** The Supplier shall document all Open-Source Software, including versions used, integrity verification, and utilize only Open-Source Software (OSS) that is current, appropriately licensed for use in Honeywell products where applicable, and free of known critical and high severity vulnerabilities at time of delivery. **12.7.4** The Supplier shall avoid to the extent possible the storage of Personally Identifiable Information (PII) within application context such as web server logs database etc. **12.7.4.1** As appropriate, leverage encryption, masking, and anonymization to meet regulatory requirements. A data dictionary (including any PII) identifying what data is included (all types) and the storage/transmission method shall be maintained. Such materials shall be provided to Honeywell as requested within 45 days' notice and shall be completed for all releases and deliveries to Honeywell. The Supplier shall participate in documenting such activities as mutually agreeable to achieve the PII regulatory compliance. **12.7.5** The Supplier shall document and perform quality cybersecurity reviews and testing. This includes vulnerability scanning and code testing, covering static, binary, and dynamic code testing on all applicable systems such as virtual machines, containers, endpoints, and executables. These tests shall adhere to current industry best practices and encompass a full range of technical testing options for all software versions before release. **12.7.5.1** The Supplier shall ensure that a basic level of penetration/security testing is performed on all products to identify risks, validate threat vectors identified in the threat model, and identify potential errors that could pose a security risk. **12.7.5.1.1** The Supplier shall document lessons learned from code testing in a searchable knowledge management system accessible to developers. **12.7.5.2** The Supplier shall analyze each vulnerability to gather sufficient information about risk to plan its remediation or other risk response.

	12.7.5.2.1 All vulnerabilities rated critical and high shall be mitigated or remediated prior to version deployment. Medium vulnerabilities shall be remediated within 90 days of discovery, and low vulnerabilities shall be remediated within 180 days of discovery. **12.7.5.2.2** Supplier shall provide cybersecurity support for the product for the duration of the warranty period agreed upon within the Master Service Agreement (MSA) or Statement of Work (SOW) whichever is greater. **12.7.5.3** The supplier shall provide a comprehensive report outlining the vulnerabilities observed during Static Code Analysis, the tool(s) used for the analysis, the methodology used for the analysis, and the ruleset(s) used for analysis. **12.7.5.3.1** The supplier shall provide a document outlining their plan for remediating any vulnerabilities found during Static Code Analysis, actions taken to remediate any vulnerabilities, and justification for any risks accepted as a result of the outcome of Static Code Analysis. **12.7.6** Production data sets shall not be used in non-production environments where the information is considered "Restricted", "Sensitive" or "Personal Data" including “Sensitive Identification Data” and “Sensitive Personal Data”. **12.7.6.1** To be considered for testing purposes, Personal Data shall be anonymized such that no personally identifiable information (PII) is included in the data set to be used for testing. **12.7.6.2** In accordance with regulatory requirements and contractual obligations, The Supplier shall gain approval from Honeywell regarding the data to be used for testing and/or developing software. **12.7.7** The Supplier shall make software integrity verification information available to Honeywell. **12.7.7.1** Providing cryptographic hashes for release files. **12.7.7.2** Use an established certificate authority for code signing.
Threat Modeling	**12.8.1** The Supplier shall perform threat modeling to identify zones conduits and the risks associated with those. **12.8.1.1** Provide the threat model to Honeywell upon request within 45 days. **12.8.1.2** Perform an attack surface evaluation. **12.8.1.3** Design in controls for any threats prioritized in the risk analysis.
Logging and Alerts for Basic Security Events	**12.9.1** The Supplier shall create and retain logs created during the testing phase to document any error checking/bug remediation. **12.9.2** Supplier shall provide a software bill of materials (SBOM) for all supplied software to include all Open Source and third-party components as documented in the National Telecommunications and Information Administration (NTIA) minimum elements for a SBOM. **12.9.3** Supplier will provide an updated SBOM for all updated versions of supplied software.
Patching & Security Updates	**12.10.1** The Supplier shall ensure that any changes made to software through patching/updates will have the ability to rollback if needed. **12.10.2** The Supplier shall proactively test and monitor for known vulnerabilities from common sources such as OWASP, Common Vulnerabilities and Exposures (CVE) , National Vulnerability Database (NVD) etc. and apply recommended patching to Product and or supporting systems as specified in integrated solution. No vulnerabilities or software errors on MITRE’s most recent Common Weakness Enumeration (CWE) Top 25 or OWASP Top Ten exist within the product. **12.10.2.1** All vulnerabilities shall be scored using Common Vulnerability Scoring System (CVSS) (CVSS 3.1 or higher) or other standard scoring framework within 15 days of discovery or notification of vulnerability. Vulnerability scoring information shall be shared with Honeywell for all critical and high vulnerabilities within 5 business days of scoring determination. **12.10.2.2** For all vulnerabilities discovered after deployment but before end-of-life, a patch will be provided for critical and high vulnerabilities within 30 days of discovery, medium vulnerabilities will be provided within 90 days of discovery and low within 180 days of discovery.
Vulnerability Management and Incident Response	**12.11.1** The Supplier shall have a process/policy in place that addresses vulnerability disclosure and remediation, and implement the roles, responsibilities, and processes needed to support that policy aligned to a current industry standard such as ISO / IEC 30111, ISO / IEC 29147. **12.11.1.1** The Supplier shall maintain documented procedures for incident response to be shared with Honeywell upon request. **12.11.1.2** The Supplier shall record lessons learned through root cause analysis in a searchable knowledge management system accessible to developers. **12.11.2** The Supplier shall notify Honeywell of confirmed cybersecurity vulnerabilities affecting Products supplied to Honeywell using the following tiered timeline:

	(a) For actively exploited vulnerabilities or severe security incidents: initial notification within twenty-four (24) hours of becoming aware, detailed vulnerability notification including affected products, versions, and available mitigations within seventy-two (72) hours, and a final report including root cause analysis and complete remediation plan within fourteen (14) days of corrective measure availability. **(b)** For confirmed Critical or High severity vulnerabilities (CVSS 7.0+) not actively exploited: notification within five (5) business days. **(c)** For confirmed Medium severity vulnerabilities (CVSS 4.0-6.9): notification within thirty (30) calendar days. Notification shall include CVE identifier (if assigned), affected product versions, severity assessment, and planned remediation timeline **12.11.3** The Supplier shall upon notification of an incident from either Honeywell, The Supplier or any third party operating similar products (and in such case when such incident is based upon software, hardware, or programmable logic in such products), The Supplier shall immediately (within 2 hours) consult with Honeywell. **12.11.4** The Supplier shall execute established and agreed upon procedures for incident reporting monitoring and tracking all security incidents until they are resolved. **12.11.5** The Supplier shall provide calling rosters (points of contact) and escalation plans to promptly investigate/address the vulnerability. **12.11.6** In the event of an incident, The Supplier shall ensure steps are immediately taken to prevent further loss and preserve the system for forensic analysis. **12.11.6.1** The Supplier shall not access or alter compromised systems. **12.11.6.2** The Supplier shall ensure preservation of system logs as electronic evidence in response to a security breach. **12.11.6.3** The Supplier shall ensure that the compromised system(s) are isolated from the network and the devices remain powered on. **12.11.6.4** The Supplier shall ensure that Honeywell is informed of the incident prior to any disclosure outside of The Supplier. **12.11.6.5** The Supplier shall notify the Honeywell focal and send a message regarding the incident to **security@honeywell.com**. The incident will contain the following information: • Date and time of incident or detection of incident • Name and contact information of person reporting the incident • Nature of the incident • Description of the event, including any Customer Confidential Information involved • Supporting evidence • More information regarding incidents upon request. **12.11.7** Any unaccounted-for documents that have been classified as Highly Confidential must be treated as a breach in security. **12.11.8** Where the Product processes Personal Data and transfers such data outside the European Economic Area, Supplier shall ensure adequate safeguards are in place in accordance with applicable data protection law and shall inform Honeywell of all countries in which Personal Data may be processed. **12.11.9** Supplier shall maintain and provide upon request a list of sub-processors that process Personal Data in connection with the Product and shall notify Honeywell of any intended changes to such list with reasonable advance notice. **12.11.10** Supplier shall provide reasonable technical and organizational assistance to enable Honeywell to fulfill data subject rights requests (access, rectification, erasure, portability) under applicable data protection law, insofar as such requests relate to Personal Data processed by the Product.
Identification and Authorization	**12.12.1** The system shall provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts by any user (human, software process or device) during a configurable time period. The system shall provide the capability to deny access for a specified period of time or until unlocked by an administrator when this limit has been exceeded. For system accounts on behalf of which critical services or servers are run, the system shall provide the capability to disallow interactive logons.
Insecure Components & Protocols	**12.13.1** The Supplier shall ensure removal of all unnecessary or insecure features components back doors files protocols ports services and methods of access before deployment. **12.13.1.1** The Supplier shall ensure that Telnet and File Transfer Protocol (FTP) protocols are not used. Where legacy compatibility requires plaintext protocols, Supplier shall document justification and implement network-level encryption (e.g., VPN tunnel).

	12.13.1.2 The Supplier shall ensure that if TLS (Transport Layer Security) is used, the minimum version is TLS 1.3. Weak cipher suites (RC4, Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), export-grade) are prohibited.
Container and Virtual Machine Scanning	**12.14.1** All Container Images and Virtual Machines (VMs) shall be scanned for vulnerabilities, malware, known secrets, and compliance checks prior to release, utilizing industry standard tools and methodologies. **12.14.1.1** For all vulnerabilities discovered a patch will be provided for CVSS scores of critical and high within 30 days medium within 90 days and low within 180 days.

Embedded Security Requirements

The following requirements apply to embedded devices and products with hardware-software integration. These controls are applicable to the specific embedded product types identified below, including devices with unidirectional connectivity, bi-directional connectivity, and fully connected embedded systems.

Section	Security Requirements Detail
Unidirectional Gateway Requirements	**12.15.1** The Supplier shall ensure the product shall not have the ability to upgrade software firmware or programmable logic.
Encryption/Cryptography	**12.16.1** Embedded devices with Non-Routable Bi-Directional Connectivity or Fully Connected devices. **12.16.1.1** The supplier shall ensure the device is provisioned with an opaque public/private key pair and a corresponding device certificate from the Honeywell Product Public Key Infrastructure (PKI) Service or other valid PKI service.

Cloud, Mobile and Automation Security

The following requirements apply based on the product deployment model: Cloud/SaaS, Mobile, and Bot/Automated Agent. Applicability is determined by the product or service type as defined in the applicability matrix.

Section	Security Requirements Detail
Identification and Authentication	**12.17.1** All administrative users and OPS have Multi-Factor Authentication (MFA) enabled. **12.17.2** The system shall provide the capability to: • Automatically enforce configurable usage restrictions • Monitor and control all methods of access via untrusted networks • Enforce usage restrictions for mobile code technologies
Mobile Application Security	**12.18.1** Supplier shall utilize **OWASP** Mobile Application Security Verification Standard (https://mas.owasp.org/) to guide the development and testing of mobile products.
Bot and Automated Agent Security	**12.19.1** The Supplier shall ensure that any bot it develops or includes in its software or product provided to Honeywell adheres to the following requirements: • Bot operations must comply with regulatory and legal requirements • Each Bot is to have unique credentials • Bot credential transmission and storage must comply with the encryption standards • Bot accounts names must be distinguishable from other account types • Bot sessions will terminate after 30 minutes of inactivity • Bot session must re-authenticate weekly or more frequently • In the event that a Bot is to perform multiple tasks against multiple systems, it shall use unique credentials for each separate system • A Bot's access is always to be limited to only what is necessary to accomplish the assigned task(s) in compliance with "Least Privileges" • Bots cannot run against systems to which any recipient is not authorized • Administrative activity is to be logged, managed and protected by a separate team • Bot CRUD events are to be logged and retained for a minimum of 30 days • Data collected during Bot operation is to be purged or removed when no longer needed for that specific operation • External cloud communication should use a Cloud Access Security broker (CASB) solution • Bots shall be designed to fail securely • Bots shall implement data validation to ensure proper processing of untrusted data • Any users that are accessing/utilizing the bots shall use MFA authentication where technically capable

Compliance and Hardware Security

The following requirements apply across all product types where applicable, including **NIST SP800-218** attestation for US Government contracts and hardware security for products containing integrated circuits or microcontrollers.

Section	Security Requirements Detail
Evidence of Compliance	**12.19.1** Upon request, Supplier shall provide attestation to the adherence of **NIST SP 800-218**. **12.19.2** Supplier shall provide evidence of cybersecurity compliance through one or more of the following certifications or attestations, as applicable to the product or service being delivered: • EU Cyber Resilience Act (Regulation (EU) 2024/2847) conformity assessment • CE Mark (where applicable to product category) • Third-party security attestations or audit reports • Capability Maturity Model Integration (CMMI) for Development • **IEC 62443-3-3**, **IEC 62443-4-1**, or **IEC 62443-4-2** certification • ISO/IEC 27001 certification
Hardware Security	**12.20.1** The Supplier shall have a documented hardware security policy for Integrated Circuits (ICs) and Microcontrollers (components which contain logic) that addresses supply chain security standards such as NIST SP 800-161 Rev1, **ISO/IEC 27001**, ISO/IEC 15408 (Common Criteria) etc. **12.20.2** The Supplier shall define a core set of security requirements for hardware security that encompasses a set of measures and standards aimed at ensuring integrity, authenticity, confidentiality, and overall security, and include it in acquisition documents, software contracts, and other agreements with third parties. **12.20.3** The Supplier shall assess suppliers, at least annually, to ensure that they are meeting the core set of security requirements defined above. **12.20.4** The Supplier shall ensure that employees and key stakeholders are trained at least annually on hardware security best practices including Secure Boot implementation, hardware-based encryption, patch and firmware management, counterfeit detections and prevention measures, etc. **12.20.5** The Supplier shall audit underlying hardware security practices, following best practices for hardware security best practices including Secure Boot implementation, hardware-based encryption, patch and firmware management, counterfeit detections and prevention measures, etc. **12.20.6** The Supplier shall review hardware security practices and procedures at a minimum annually and update as needed to ensure industry best practices are being addressed. **12.20.7** The Supplier shall require third-party suppliers of hardware to provide documentation, such as a Certificate of Authenticity (COA), Bill of Materials (BOM), Certificate of Compliance (COC), as documentation of authenticity of their products.

Artificial Intelligence and Machine Learning

The following requirements apply when the product or service involves AI/ML capabilities, including model development, training, deployment, and ongoing monitoring.

Section	Security Requirements Detail
AI: AI Governance and Risk Management	**12.22.1** AI models must be restricted to the minimum set of data and permissions to fulfil their intended purposes. **12.22.2** Supplier shall identify and document AI-specific risks relevant to Products supplied to Honeywell, the controls in place to mitigate them, and shall communicate these risks and potential impacts to Honeywell. **12.22.3** Supplier shall assess and document the likelihood and potential impact of AI-related risks for Products supplied to Honeywell. **12.22.4** No AI model is permitted to influence systems or services that impact life safety. **12.22.5** AI models that have reached end-of-support from their originating vendor or open-source project, or that have known unpatched vulnerabilities, shall not be deployed in Products supplied to Honeywell. **12.22.5.1** AI model application logic and architecture must comply with the applicable Product Security requirements set forth in this document. **12.22.6** For approved HR use cases, AI models must have bias detection and mitigation (i.e., regular audits which validate fairness, transparency, and model decision interpretability).

AI: AI Development and Testing	**12.23.1** AI components shall be developed for and restricted to use cases documented in the applicable SOW or product specification agreed upon with Honeywell. **12.23.1.1** For each AI model, a statement of the intended and appropriate use shall be developed and made available to all users of the AI model. Users must acknowledge the statement of use before consuming the AI model service. **12.23.2** Training data shall be protected in accordance with the most sensitive classification in scope, including protection against training data poisoning and extraction attacks. **12.23.3** Where the Product accepts natural language or user-generated inputs, Supplier shall implement content filtering to detect and handle adversarial or inappropriate inputs.
AI: AI Code Review and Operations	**12.24.1** AI-generated code incorporated into Products shall undergo code review by two (2) or more qualified persons independent of the original development prior to deployment. **12.24.2** AI applications shall have a penetration test completed prior to release to customer or production, including adversarial Machine Learning (ML) testing such as model evasion, data poisoning, and model extraction where applicable.
AI: AI Monitoring and Drift Detection	**12.25.1** Supplier shall periodically review the access permissions under which an AI-powered application operates, with particular attention to data access scope expansion and model capability drift. **12.25.2** Training and reference data shall be validated for accuracy, relevance, and absence of unauthorized content prior to use and periodically thereafter. **12.25.3** Continuous monitoring shall be enabled to detect model drift, anomalous outputs, adversarial inputs, and security incidents. **12.25.4** A log of irregular responses, security incidents, and unusual AI model behavior shall be retained and made available to Honeywell on request.
AI: AI Data Protection and Privacy	**12.26.1** Honeywell data collected by a third-party cannot be shared or sold without explicit permission and documented in a procurement agreement. **12.26.2** Supplier shall comply with applicable legal and regulatory requirements (such as NIST AI Risk Management Framework (RMF) or **ISO 42001**) related to AI, including a process to complete an AI risk assessment for Products supplied to Honeywell. **12.26.3** Supplier shall establish and maintain procedures for safely decommissioning AI components in Products supplied to Honeywell, including secure deletion of training data and model artifacts. **12.26.3.1** Supplier shall establish and maintain a centralized inventory of AI-powered applications and services provided to Honeywell. **12.26.4** Supplier shall ensure accountability structures are in place with the appropriate individuals responsible and trained for mapping, measuring, and managing AI risks. **12.26.5** Supplier shall establish and maintain processes and procedures that define and differentiate roles and responsibilities for human-AI configurations and oversight of AI systems.
AI: AI Model Integrity and Supply Chain	**12.27.1** Supplier shall track the provenance of training data used for AI models in Products supplied to Honeywell and shall make provenance documentation available upon request under Non-Disclosure Agreement (NDA). **12.27.2** Supplier shall maintain attestations of training dataset integrity and provenance. Where industry-standard AI/ML bill of materials formats are available, Supplier shall provide such documentation. **12.27.3** Supplier shall test AI models against adversarial samples and implement appropriate guardrails on the use of training and testing data to evaluate model robustness. **12.27.4** Where AI models are trained on sensitive data (PCI, Protected Health Information (PHI), PII), Supplier shall implement access controls on the resulting model commensurate with the sensitivity of the training data. **12.27.5** Supplier shall document, to the extent reasonable and without requiring disclosure of proprietary methodologies, the training process for AI models including data sources, preprocessing steps, and security controls applied during training.
AI: AI Transparency and Disclosure	**12.28.1** Supplier shall provide documentation of known AI model limitations, confidence boundaries, and failure modes, along with instructions for reporting cybersecurity or safety concerns. **12.28.2** Supplier shall disclose provenance of training, fine-tuning, and alignment data to Honeywell upon request under NDA. **12.28.3** Supplier shall establish documented criteria and procedures for when to stop using, degrade, or roll back an AI model in Products supplied to Honeywell, including procedures for compromised or degraded models.

COTS: Vendor Obligations and Lifecycle

The following requirements define vendor commitments for COTS products procured by Honeywell, including software composition transparency, product lifecycle support, vulnerability disclosure, secure update distribution, vendor assessment, and business continuity.

Section	Security Requirements Detail
COTS: Software Bill of Materials (SBOM)	**12.29.1** Supplier shall provide an SBOM for all supplied software. **12.29.2** The SBOM shall be provided in Software Package Data Exchange (SPDX) 2.3+ or CycloneDX 1.4+ format and shall be kept current to reflect the composition of the delivered product. **12.29.3** Products shall be clearly identifiable by product name, type designation, batch or serial number (where applicable), and software version number. Software products shall include a machine-readable version identifier accessible to the user or integrator.
COTS: Product Lifecycle Management	**12.30.1** Supplier shall notify Honeywell a minimum of twelve (12) months in advance of any product end-of-life or end-of-support date. Notification shall include: • planned End of Life (EOL)/EOS dates • duration of any extended support offering • recommended migration paths to successor products • the date of the final security patch **12.30.2** Supplier shall publish and maintain a version support matrix listing all currently supported product versions, the date each version reaches end-of-security-support, and whether each version receives feature updates or security-only updates. The matrix shall be updated within thirty (30) days of any version release or support status change. **12.30.3** For any product version reaching end-of-life, Supplier shall provide a final security notice summarizing known unpatched vulnerabilities, recommended compensating controls, and available extended-support or migration options.
COTS: Vulnerability Disclosure and Advisory	**12.31.1** Supplier shall maintain a customer-accessible security advisory portal that publishes security advisories including CVE identifiers, CVSS scores, affected product versions, available patches or workarounds, and recommended remediation timelines. Advisories shall be published within seventy-two (72) hours of patch availability. **12.31.2** Supplier shall notify Honeywell within twenty-four (24) hours of confirmation of any security breach affecting products delivered to Honeywell, including supply chain compromise, build system breach, or code signing key compromise. Notification shall include the nature of the breach, affected products and versions, and immediate recommended actions. Supplier shall provide ongoing updates at intervals no greater than every seven (7) calendar days until resolution. Notification may be fulfilled through direct communication or public advisory to all affected customers. **12.31.3** Supplier shall participate in relevant industry vulnerability information sharing programs (e.g., ISACs, Computer Emergency Response Team (CERT) coordination) as applicable to the product domain. Supplier shall not restrict Honeywell from sharing vulnerability information with affected parties or regulatory authorities as required by applicable law.
COTS: Secure Update Distribution	**12.32.1** Supplier shall provide security patches at no additional charge for all supported product versions throughout the declared support period. Patches shall be available for download within forty-eight (48) hours of public release **12.32.2** Supplier shall conduct regular security testing of the product, including at minimum: vulnerability scanning prior to each release, and periodic penetration testing or independent security review at least annually for products under active support. Summary results of security testing shall be available to Honeywell upon request.
COTS: COTS Vendor Assessment	**12.33.1** Supplier shall complete a Honeywell COTS vendor security assessment questionnaire covering: • SDLC maturity (BSIMM • Software Assurance Maturity Model (SAMM) • IEC 62443-4-1 certification level) • security incident history for the prior twenty-four (24) months • current audit certifications (SOC 2 Type II, ISO 27001, ISASecure) • security team structure • supply chain security practices. The assessment shall be repeated annually or upon material change **12.33.2** For products deployed in safety-critical or high-security environments, Supplier shall obtain independent third-party security certification such as ISASecure Embedded Device Security Assurance

	(EDSA)/SSA/SDLA, **IEC 62443-4-1** (minimum Maturity Level 2), **IEC 62443-4-2** (minimum Security Level 2), or an equivalent recognized certification. Supplier shall disclose certification status and expiration dates. **12.33.3** Supplier shall provide and maintain current manufacturer identification including: • legal entity name • registered trade name or trademark • postal address • a dedicated email address for security-related communications. Where the product is manufactured by a third party on behalf of the Supplier, the Supplier shall disclose the manufacturer identity
COTS: Compatibility and Business Continuity	**12.34.1** For critical COTS software, Supplier shall establish a source code escrow arrangement with an independent third-party escrow agent. Release conditions shall include: Supplier insolvency, material breach of support obligations, product discontinuation without a viable migration path, or acquisition by a sanctioned entity. Escrow contents shall be updated with each major product release. **12.34.2** Supplier shall publish and maintain a compatibility matrix listing supported operating systems, platforms, and integration interfaces for each product version. Supplier shall provide a minimum of ninety (90) days advance notification of any update that may affect interoperability with existing systems or require changes to the customer environment.

COTS: Product Configuration and Delivery

The following requirements specify the expected state of COTS products at delivery, including secure default configurations, secure data removal capabilities, and product documentation and transparency.

Section	Security Requirements Detail
COTS: Secure Data Removal	**12.35.1** Products shall process only data that is adequate, relevant, and limited to what is necessary for the intended functionality. Products shall not collect, transmit, or store data beyond what is required for their documented purpose. Where personal data is processed, the product shall support data minimization consistent with applicable data protection regulations.
COTS: Product Documentation and Transparency	**12.36.1** Product documentation shall identify where to obtain further security information including: the Supplier's security advisory portal, vulnerability reporting mechanism, SBOM location, and applicable security certifications.

COTS: Technical Security Requirements

The following requirements define the technical security capabilities that COTS products must provide, including authentication, cryptography, audit logging, integrity and resilience, network security, and regulatory conformity.

Section	Security Requirements Detail
COTS: Cryptography	**12.37.1** Products shall protect the confidentiality of stored, transmitted, and processed data using cryptographic mechanisms. Data at rest shall be encrypted using AES-256 or equivalent. Data in transit shall be protected using current versions of TLS. TLS 1.3 to be supported for all data in transit. If TLS 1.2 must be supported, and not yet globally yet deprecated, disable obsolete cipher suites and enforce modern, strong algorithms (such as ECDHE for key exchange and AES-GCM for encryption). **12.37.2** Products shall not use deprecated or broken cryptographic algorithms including but not limited to: • Message Digest Algorithm 5 (MD5) or Secure Hash Algorithm (SHA)-1 for digital signatures or integrity verification • DES, 3DES • RC4 for encryption • Rivest-Shamir-Adleman (RSA) key sizes below 2048 bits **12.37.3** Products shall implement key management practices consistent with industry standards (e.g., **NIST SP 800-57**). Cryptographic keys shall be generated using approved random number generators, stored in secure storage (hardware security module, Trusted Platform Module (TPM), or secure enclave where available), and rotatable without requiring product reinstallation. **12.37.4** Products shall not use Telnet, FTP, or other plaintext protocols for any communication carrying authentication credentials, configuration data, or sensitive information. Where legacy compatibility requires plaintext protocols, Supplier shall document justification and implement network-level encryption (e.g., VPN tunnel).

COTS: Audit Logging and Monitoring	**12.38.1** Products shall provide the capability to generate audit records for security-relevant events including: authentication successes and failures, authorization decisions, configuration changes, firmware and software updates, administrative actions, and security-relevant errors. **12.38.2** Audit log timestamps shall use Coordinated Universal Time (UTC) with millisecond precision where supported by the platform. Products shall support time synchronization via Network Time Protocol (NTP) or Precision Time Protocol (PTP) to ensure log timestamp accuracy and correlation across systems. **12.38.3** Products shall support export of audit logs in at least one industry-standard format (syslog per RFC 5424, Common Event Format (CEF), or structured JSON) to enable integration with external security information and event management (SIEM) systems. **12.38.4** Products shall allocate sufficient audit log storage capacity according to commonly recognized recommendations. Products shall provide configurable behavior when storage capacity is approaching exhaustion, including: overwrite-oldest, stop-logging with alert, or alert-when-full notification to administrators.
COTS: Integrity and Resilience	**12.39.1** Supplier shall make software integrity verification information available to Honeywell, including cryptographic hashes for release files and code signing verification instructions.
COTS: Regulatory Conformity Recognition	**12.40.1** Where a product holds a valid certification or declaration of conformity under a recognized cybersecurity regulation or scheme (e.g., EU Cyber Resilience Act conformity per Regulation 2024/2847, **IEC 62443-4-2** component certification, or equivalent national scheme), Supplier may present such certification as evidence of compliance with the corresponding technical requirements in the corresponding COTS technical requirements in section 12 of this document. Honeywell reserves the right to review the scope and validity of the certification to confirm it addresses the applicable requirements. **12.40.2** Acceptable evidence of regulatory conformity shall include: an EU Declaration of Conformity, an EU-type examination certificate from a notified body, a certificate under an applicable cybersecurity certification scheme (e.g., European Union Common Criteria (EUCC), IEC 62443), or an equivalent third-party assessment report. Self-declarations without supporting third-party evidence are not sufficient. **12.40.3** Regulatory conformity evidence shall satisfy only those requirements that map to a specific obligation within the recognized regulation or scheme. Requirements in this contract that exceed the scope of the regulation, including but not limited to Service Level Agreement (SLA) response times, escrow provisions, SBOM format specifications, and Honeywell-specific reporting obligations, remain independently applicable regardless of conformity status. **12.40.4** Supplier shall notify Honeywell within thirty (30) calendar days if a product's regulatory conformity status changes, including withdrawal of a declaration of conformity, expiration of a certification, identification of an actively exploited vulnerability requiring updated conformity assessment, or a change in the regulatory classification of the product.

13. Remote Network Access

Applicability: This section applies when Supplier personnel require remote login access to Honeywell or customer networks using Honeywell-managed identifiers (EID/HID), including Virtual Private Network (VPN), remote desktop, and other remote connectivity methods.

Section	Security Requirements Detail
Remote Network Access to Honeywell Network	**13.1.1** Remotely accessing Honeywell resources, using Honeywell electronic identifiers (EID/HID) which Supplier agrees to collaborate with Honeywell or the designated MSP to generate, is restricted to Honeywell-managed equipment, Honeywell's virtual desktop image (VDI) offering for non-Honeywell managed Windows-based equipment or Mac Kickstart offering for Mac-based equipment. **13.1.2** The minimum systems requirements for Honeywell's VDI solution are: **13.1.3** Microsoft Windows OS or Apple Mac OS device using supported OS-specific remote desktop client; **13.1.4** Minimum network bandwidth of 3 Megabits per second (Mbps) and; **13.1.5** Network latency below 100 milliseconds (ms).

14. Shipping Security

Applicability: This section applies when the Supplier is involved in the physical shipping or transport of Honeywell products, materials, or components through the supply chain, or handles hazardous chemicals in connection with Honeywell deliverables.

Section	Security Requirements Detail
Honeywell Physical Product Transport	**14.1.1** Supplier will use commercially reasonable efforts to maintain certification under the Business Partner Criteria of any Supply Chain Security Program that the country of import for the Goods may adopt such as the U.S. Customs-Trade Partnership Against Terrorism (CTPAT) or other World Customs Organization (WCO) sanctioned supply chain security program. Supplier will **(i)** advise Honeywell of the specific Supply Chain Security Program and **(ii)** authorize certification monitoring by Honeywell. **14.1.2** If Supplier is not certified by a WCO-sanctioned program, then Supplier will: **14.1.3** adhere to the security criteria for Supplier's applicable CTPAT category (e.g., Importer, Foreign Manufacturer, etc.); and **14.1.4** upon Honeywell's request, complete an annual survey attesting to its compliance with a WCO-sanctioned program. For reference: • CTPAT security criteria requirements are located at http://www.cbp.gov/border-security/ports-entry/cargo-security/CTPAT-customs-trade-partnership-against-terrorism/apply/security-criteria • AEO requirements are located at https://ec.europa.eu/taxation_customs/general-information-customs/customs-security/authorised-economic-operator-aeo_en • PIP requirements are located at https://www.cbsa-asfc.gc.ca/services/security-securite/business-affaires/ttp-pndc/pip-pep/menu-eng.html • For other WCO programs that are country-specific, please contact your local import compliance contact or customs official
Hazardous Chemical Transport	**14.2.1** Supplier will maintain an appropriate shipping security program to maintain compliance with applicable regulatory requirements, which may include ChemLock program and 49 CFR. For reference: • ChemLock program: https://www.cisa.gov/resources-tools/programs/chemlock • 49 CFR Parts 171-177: Hazardous Materials Regulations: https://www.ecfr.gov/current/title-49/subtitle-B/chapter-I/subchapter-C/part-171

15. Supplier Facility Security

Applicability: This section applies when the Supplier manages IT assets, devices, or equipment used to process, store, or access Honeywell Confidential Information.

Supplier shall comply with the applicable facility security requirements of **NIST SP 800-53 Rev. 5** or the equivalent controls of **ISO/IEC 27001:2022**. The following supplemental requirements apply.

Section	Security Requirements Detail
Supplier Physical and Environmental Security	**15.1.1** Supplier shall assess the effectiveness of security controls at Supplier alternate work sites on a periodic basis based on risk (not to exceed one year).
Physical Access Monitoring	**15.2.1** Supplier shall maintain physical access logs to its facilities and retain these logs for at least 180 days.
Visitor Management	**15.3.1** Supplier shall maintain records (at least 180 days) of visitor access to the facilities and review visitor access records at least monthly and take appropriate measures. **15.3.2** Supplier will regularly review and update access rights of their personnel to facilities housing Customer Confidential Information and that when such personnel no longer provide services to Honeywell, access is removed within one (1) business day, except in urgent situations where access removal should be immediate. **15.3.3** Supplier shall ensure that only authorized persons are allowed unescorted access to its facilities having access to Honeywell resources. **15.3.4** Supplier shall review the list of individuals that have physical access to facilities, on a periodic basis (not to exceed six (6) months) and take measures as appropriate. **15.3.5** Supplier shall revoke physical access rights provided to personnel upon termination as soon as possible (not to exceed one business day). This shall include disabling of physical access mechanisms such as keys or access cards.
Environmental Security: Data Centers and Information Processing Facilities	**15.4.1** Supplier shall maintain the following controls: ○ Fire detection and suppression in data processing facilities; ○ Temperature and humidity controls; ○ Power equipment and cabling protection; ○ Emergency shutoff switches in accessible areas; ○ UPS for orderly shutdown or continuous running; ○ Emergency lighting for evacuation routes; ○ Regular monitoring and maintenance of data center utilities; ○ Annual data center fire drills.

16. Definitions

AI Model: A computational model that uses machine learning algorithms trained on data to perform tasks such as classification, prediction, generation, or decision-making.

AME (Advanced Manufacturing Engineer): A Honeywell engineering role responsible for manufacturing process design, optimization, and operational technology (OT) systems at Honeywell production facilities. The designated AME site contact receives priority incident notifications for OT environment events.

Audit Log: A chronological record of security-relevant events, including user access, system changes, authentication attempts, and administrative actions, maintained to support accountability, forensic investigation, and compliance verification.

Cipher Suite: A set of cryptographic algorithms used together to secure a network connection, typically specifying the key exchange algorithm, bulk encryption algorithm, and message authentication code (MAC). Weak or deprecated cipher suites (e.g., RC4, DES, 3DES, export-grade) shall not be used.

CIS (Center for Internet Security): A nonprofit organization that publishes security configuration benchmarks for operating systems, cloud platforms, network devices, and applications. CIS Benchmarks define tiered hardening levels (Level 1 and Level 2) used as baselines for secure system configuration.

Conduit: A logical or physical grouping of communication channels connecting two or more zones that share common security requirements, as defined in IEC 62443. Conduits control and monitor data flow between zones.

Confidential Information: Any non-public information disclosed by Honeywell to the Supplier, including but not limited to technical data, trade secrets, business plans, financial information, and proprietary software.

Customer Confidential Information: Any non-public information disclosed by Honeywell to the Supplier, including but not limited to technical data, trade secrets, business plans, financial information, and proprietary software of Honeywell or its customers.

COTS (Commercial Off-The-Shelf): A product, including software, firmware, or hardware, that is commercially available, sold in substantial quantities, and provided to Honeywell as a finished good without custom modification.

CUI (Controlled Unclassified Information): Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act. CUI includes Covered Defense Information (CDI) and Federal Contract Information (FCI).

CVSS (Common Vulnerability Scoring System): An open industry standard for assessing the severity of computer system security vulnerabilities on a scale of 0.0 to 10.0, where Critical (9.0-10.0), High (7.0-8.9), Medium (4.0-6.9), and Low (0.1-3.9) ratings determine remediation SLA timelines under this agreement.

Cybersecurity Incident: An event that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation of security policies, procedures, or acceptable use policies.

End-of-Life (EOL): The date after which a product, software version, or component is no longer supported by the Supplier with security patches, updates, or technical assistance. Supplier shall provide advance notice of EOL dates as specified in the applicable requirements.

Escrow: An arrangement in which source code, build tools, documentation, or other critical assets are deposited with an independent third party, to be released to Honeywell upon the occurrence of specified trigger events such as Supplier bankruptcy, discontinuation of the product, or failure to provide contracted support.

Export Controlled: Information, technical data, software, or technology subject to export control regulations including the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). Transfer of export-controlled items to foreign persons or destinations requires prior government authorization.

FAT (Factory Acceptance Test): A formal test performed at the manufacturer's or supplier's facility to verify that a product, system, or component meets specified requirements and performance criteria before shipment to the customer site.

Firmware: Software that is embedded in a hardware device, typically stored in non-volatile memory (e.g., ROM, flash), that provides low-level control and operational instructions for the device. Firmware updates may be delivered as part of product security patches.

Honeywell Information Resources: All Honeywell-owned or Honeywell-managed information technology assets, including networks, systems, applications, and data, regardless of location or hosting arrangement.

IACS (Industrial Automation and Control Systems): Systems used for industrial process control and automation, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and programmable logic controllers (PLC).

Least Privilege: The security principle that any user, process, or system component is granted only the minimum access rights and permissions necessary to perform its authorized function, and no more.

MFA (Multi-Factor Authentication): An authentication method requiring two or more independent verification factors: something the user knows (password), something the user has (token, smart card), or something the user is (biometric). MFA is required for privileged access and remote access as specified in the applicable requirements.

MSP: Managed Service Provider

Model Weights: The learned parameters of an AI model that encode the knowledge acquired during training. Model weights are considered high-value intellectual property requiring protection from unauthorized access and modification.

Operational Technology (OT): Hardware and software that detects or causes a change through the direct monitoring and control of industrial equipment, assets, processes, and events. OT includes SCADA systems, distributed control systems, programmable logic controllers, and other industrial automation components.

PASTA (Process for Attack Simulation and Threat Analysis): A risk-centric threat modeling methodology that aligns business objectives with technical requirements through a seven-stage process to identify, enumerate, and score threats based on attack likelihood and business impact.

PCI (Payment Card Industry): Refers to PCI DSS (Payment Card Industry Data Security Standard), a set of security requirements for organizations that handle branded credit cards. Products or services processing, storing, or transmitting cardholder data must comply with applicable PCI DSS requirements.

Penetration Test: An authorized simulated cyberattack on a computer system or network, performed to evaluate the security of the system by actively exploiting vulnerabilities.

PHI (Protected Health Information): Individually identifiable health information, including demographic data, medical histories, test results, insurance information, and other data collected by a healthcare provider or plan, that is protected under HIPAA and applicable regulations.

PII (Personally Identifiable Information): Information that can be used to identify, contact, or locate an individual, either alone or when combined with other data. Includes but is not limited to name, address, Social Security number, email address, biometric data, and IP address when linked to an individual.

Processing: Any operation or set of operations performed on data or information, including collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment, combination, restriction, erasure, or destruction.

Product: Any software, hardware, firmware, system, service, or combination thereof provided by the Supplier to Honeywell under this agreement, including all components, updates, patches, and associated documentation. Where the context requires, Product includes COTS products, custom-developed solutions, cloud-hosted services, and AI-enabled systems.

Provenance: The documented origin, history, and chain of custody of data, software components, AI models, or artifacts throughout their lifecycle.

RFC 5424: The Internet Engineering Task Force (IETF) standard defining the syslog protocol for transmitting event notification messages across IP networks. Used as the format specification for forwarding audit logs to centralized logging services.

Risk Assessment: A systematic process for identifying, analyzing, and evaluating risks to organizational operations, assets, individuals, and other organizations.

RPO (Recovery Point Objective): The maximum acceptable amount of data loss measured in time. RPO defines the point in time to which data must be recovered after a disruption (e.g., an RPO of 4 hours means no more than 4 hours of data may be lost).

RTO (Recovery Time Objective): The maximum acceptable duration of time within which a system, service, or process must be restored after a disruption before unacceptable consequences occur.

SAT (Site Acceptance Test): A formal test performed at the customer's site after installation to verify that a product, system, or component operates correctly in its intended environment and meets all specified requirements.

SBOM (Software Bill of Materials): A formal, machine-readable inventory of software components and dependencies, their relationships, and their hierarchical structure within a product.

SDLC (Software Development Lifecycle): A structured process for planning, creating, testing, deploying, and maintaining software applications, including secure development practices.

Secure Boot: A security mechanism that ensures a device boots using only software that is trusted and cryptographically verified by the manufacturer or authorized entity, preventing unauthorized or tampered firmware from executing during startup.

SLA (Service Level Agreement): A documented commitment between Supplier and Honeywell that defines measurable performance and response targets, including but not limited to vulnerability remediation timelines, incident response times, uptime guarantees, and support availability.

SSDLC (Secure Software Development Lifecycle): An SDLC that integrates security practices at every phase, including threat modeling, secure coding, security testing, and vulnerability management.

STRIDE: A threat modeling methodology that categorizes threats into six types: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. Used during the design phase to systematically identify potential security threats.

Supplier: Any third-party organization, vendor, contractor, or service provider that provides products, services, or access to systems on behalf of or in connection with Honeywell.

Technical Information: Information, including research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, and related information, that can be used or adapted for use in the design, production, manufacture, utilization, or reconstruction of articles or materials.

Third Party (Supplier): Any third-party organization, vendor, contractor, or service provider that provides products, services, or access to systems on behalf of or in connection with Honeywell under the terms of this agreement.

Third Party Information Systems: Information systems or components thereof that are owned, operated, or maintained by a third party and used to process, store, or transmit Honeywell information or provide services to Honeywell.

Third Party Materials: Any software, hardware, firmware, documentation, data, or other materials provided by or originating from a third party that are incorporated into or used in connection with products or services delivered to Honeywell.

Third Party Personnel: Any individual employed by, contracted to, or otherwise acting on behalf of a third party who performs work, provides services, or accesses Honeywell information resources or facilities in connection with this agreement.

Third-Party: Any entity other than Honeywell and the Supplier, including sub-suppliers, subcontractors, open-source software maintainers, cloud infrastructure providers, and any other external party whose products, services, or components are incorporated into or support the Product.

Training Data: The dataset used to train an AI model, including all data used for initial training, fine-tuning, alignment, and testing purposes.

Trusted Third Party Network Connection: A network connection between Honeywell and a third party that has been formally approved, documented, and secured in accordance with Honeywell network security requirements, including appropriate access controls, encryption, monitoring, and periodic review.

Vulnerability: A weakness in an information system, system security procedure, internal control, or implementation that could be exploited by a threat source.

Vulnerability Disclosure: The process by which security vulnerabilities are reported, tracked, and communicated to affected parties. Coordinated vulnerability disclosure follows established timelines and notification procedures to allow remediation before public release of vulnerability details.

Zone: A logical or physical grouping of assets that share common security requirements, as defined in IEC 62443. Zones establish security boundaries within which a consistent set of security policies are applied.

17. Service Type Definitions

Cloud Service – Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS): Suppliers providing cloud-based computing resources or applications. IaaS suppliers deliver virtualized infrastructure (compute, storage, networking). PaaS suppliers provide development and deployment platforms on which Honeywell builds or runs applications. SaaS suppliers deliver fully managed software applications accessed over the internet. These suppliers typically process, store, or transmit Honeywell data within their cloud environments, making them subject to elevated data protection and access control requirements.
Co-lo – No Access to HON Data: Suppliers operating colocation data center facilities where Honeywell houses its own physical servers and networking equipment. The supplier provides power, cooling, physical space, and physical security, but does not have logical access to Honeywell data or systems hosted within the colocation environment.
Consultant / Sales Representative: External individuals or firms engaged to provide advisory, professional, or sales-related services on behalf of or to Honeywell. This category covers management consultants, technical advisors, staff augmentation resources, and third-party sales agents.
Data Transport: Suppliers responsible for the electronic transmission of Honeywell data between locations or systems. This includes Internet Service Providers (ISP)s, managed file transfer providers, and network transport carriers.
External IP – No Hosting: Suppliers that receive Honeywell intellectual property that is managed within their internal environment, but don't provide any internet-facing/Cloud Service to Honeywell. Examples include insurance companies, engineering companies, and similar.
Manufacturing – Hardware Only: Suppliers that manufacture physical hardware components or finished goods for Honeywell products, with no software, firmware, or embedded logic involved. Examples include mechanical parts, enclosures, circuit boards (unprogrammed), and raw materials fabrication.
Manufacturing – Hardware & Software: Suppliers that manufacture products containing both hardware and embedded software or firmware for Honeywell. This includes programmable controllers, sensor modules with onboard logic, and assembled units with pre-loaded operating systems, whether or not customize for Honeywell.
Manufacturing – Low Risk: Suppliers providing manufactured goods that present minimal cybersecurity or data exposure risk to Honeywell. Typical examples include Commercial Off-The-Shelf (COTS) products, or those where only low risk information was shared in order to manufacture such product and if the information shared is compromised, very limited harm to Honeywell would occur.
On Site Access – With Network Access: Suppliers whose personnel require physical presence at a Honeywell facility and connectivity to Honeywell's internal network to perform their work. Examples include IT service technicians, system integrators, and building automation contractors.
On Site Access – Without Network Access: Suppliers whose personnel require unescorted badge access at a Honeywell facility but do not need or receive any connectivity to Honeywell networks. Examples include janitorial staff, food service providers, construction contractors, and equipment maintenance crews.
Product Development – COTS: Suppliers providing Commercial Off-The-Shelf (COTS) products that Honeywell integrates into its own solutions or uses internally. These are standard, pre-built products sold to the general market without Honeywell-specific customization.
Product Development – Custom: Suppliers engaged to develop bespoke products, software, or solutions built to Honeywell's specifications. This includes custom application development, purpose-built firmware, and engineered-to-order hardware. These engagements typically involve deeper access to Honeywell IP, design documentation, and technical environments, requiring strong controls around secure development practices, code review, IP protection, and access governance.
Remote Network Access: Suppliers that connect to Honeywell's internal networks remotely (e.g., via VPN or Honeywell issued laptop) to provide support, monitoring, or management services. Examples include managed security service providers, remote IT support, and industrial control system monitoring. Key risk areas include credential management, session monitoring, least-privilege access enforcement, and endpoint security validation for the supplier's connecting devices.
Shipping Only: Suppliers limited to the physical transport and delivery of goods to or from Honeywell facilities. These suppliers handle packaged shipments but do not open, inspect, or interact with the product contents and have no access to Honeywell data or networks.
Transportation / Lodging: Suppliers providing travel and accommodation services for Honeywell personnel. This includes airlines, car rental companies, shuttle companies, hotels, and corporate travel management agencies. While these suppliers generally do not access Honeywell technical systems, they may process personal data of Honeywell employees (names, travel itineraries, payment information).
Warehouse Management – Supplier Facility: Suppliers that store, handle, or manage Honeywell inventory or materials at the supplier's own warehouse facility. This includes third-party logistics (3PL) providers and contract warehousing operations.

18. Revision History

Effective Date	Version	Description of Change	Section(s) Impacted
8/3/2026	1.0	Initial Release	All