Honeywell

HONEYWELL BUILDING TECHNOLOGIES
buildings.honeywell.com

HONEYWELL GOVERNING SECURITY TERMS AND CONDITIONS

The Honeywell Security Terms and Conditions for Suppliers set out below ("Security Terms and Conditions") were determined based on the anticipated scope of Services and Deliverables. If there is a subsequent change to scope of Services of Deliverables to be provided under this Agreement that impacts the previously agreed upon Security Terms and Conditions, then the Parties shall agree to amend this Security Terms and Conditions to reflect such change appropriately.

The Security Terms and Conditions are based on Honeywell's Global Security Policies and Standards and may be modified from time to time. However, Honeywell will provide written notice to Supplier thirty (30) days in advance for any modification that impacts Supplier and no modification that has a material cost or other impact to Supplier will be effective until agreed to in writing by Supplier.

Security Terms and Conditions

Supplier		Honeywell Procurement	
Date	9/30/2019 16:55	Honeywell Sponsor	

Purpose
The purpose of these Security Terms and Conditions is to advance Honeywell's technical and physical security, management, support, access, monitoring and compliance requirements for work performed on its behalf. It is imperative that all supplier relationships are formalized to include continuity of service and auditing of those services.

Scope
Supplier shall mean the legal entity defined as such in the Agreement or, if not expressly defined, the legal entity entering into the Agreement to provide goods or services to Honeywell to which these Security Terms and Conditions shall apply. The Supplier shall be responsible to ensure compliance with these Security Terms, including the compliance of all of its subsidiaries, affiliates, and (sub)contractors involved by Supplier in providing the goods or services to Honeywell.

Please note: the content for these Security Terms and Conditions is taken from a collection of Honeywell security policies and standards. The numbering scheme for certain sections of this document is such that 4.x denotes "Policy" level items while 5.x denotes corresponding Standard/Procedural items. For example, procedural item 5.6.2 corresponds to policy item 4.6.2.

Category	Applicable Requirements
Product Development Security	6.0 Product Development Security If any goods, products, software, services or deliverables (collectively, "Products") supplied under this Agreement include executable code, Supplier agrees to comply with the requirements set forth in this section. 6.1 Product Development Environment Supplier shall establish and maintain cybersecurity safeguards meeting current industry best practices

	to ensure that the confidentiality, integrity, and availability of the development and production environments supporting the Product (e.g. IEC62443, CSA). 6.1.1 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). 6.1.2 Application development and test environments shall be physically or logically separated from the production environments (network, servers or databases). 6.2. Product Development 6.2.1 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 OWASP, CSA, IEC62443 and regulatory requirements, including, security design review, secure coding practices, risk-based testing and remediation requirements. 6.2.1.1 Supplier shall remove unnecessary features, components, files, protocols, and ports. 6.2.1.2 Supplier shall register all Open Source Software, document versions, and utilize only OSS that is current, appropriately licensed for use by Honeywell, and free of defects 6.2.1.3 Supplier shall complete and provide to Honeywell a threat model based on the STRIDE method, a data flow diagram, and risk assessment for any product delivered to Honeywell upon request within 45 days. 6.2.1.4 Supplier shall track the creation, reading, updating and deletion (CRUD) of events for common logs. 6.2.1.5 Supplier shall log all security relevant events including, as a minimum: Failed logons, Account lockouts, Logon times, Log tampering and deletion, and Failed object access events High security events over time. These logs shall be retained according to the industry and or legal standards set forth for the environment and purpose, not to be less than 90 days. 6.2.2 Supplier shall provide training on secure coding principles and awareness of industry standards to personnel involved in the development and coding of Products. The training shall be given at least annually to Supplier personnel and subcontractors and include comprehension validation. 6.2.3 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. As appropriate, leverage encryption, masking and anonymization to meet regulatory requirements. A PII data dictionary identifying what data is included (all types), the storage/transmission method, and a PII questionnaire from Honeywell must be complmeted for all releases and deliveries to Honeywell. 6.2.4 The Supplier must provide mechanisms to encrypt the all data in transit and at rest, based on the sensitivity of data, within the product and for all connection methods. 6.2.5 Supplier shall develop and maintain an up-to-date cybersecurity vulnerability management plan designed to promptly identify, prevent, investigate, and mitigate any cybersecurity vulnerabilities and shall complete vulnerability analysis (both automated and manual) and perform any required recovery actions to remedy the impact 6.2.6 Supplier ensure a process is in place to include incident response and emergency response where that process is aligned with current industry standard (e.g., ISO / IEC 30111, ISO / IEC 29147). 6.2.6.1 Supplier shall notify Honeywell within five (5) business days after discovery, or shorter if required by applicable law or regulation, of any potential cybersecurity vulnerability. 6.3 Product Testing 6.3.1 Supplier shall document and perform quality and cybersecurity reviews and testing, including vulnerability scanning covering static, dynamic, and secure code testing using current industry best

	practices with full scope of technical testing options for all versions of software prior to release. 6.3.1.1 All vulnerabilities rated high and medium shall be remediated prior to version deployment. 6.3.2 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”. 6.3.2.1 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. 6.3.2.2 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. 6.4 Product Maintenance 6.4.1. Supplier software products and services are to maintain up-to-date security patches as applicable and in accordance with industry recommendations, and delivered in no less than 45 days of date notified to Supplier by any party; 6.4.2. Supplier will provide security updates as applicable for products under maintenance. 6.4.3 Supplier shall monitor for known vulnerabilities from common sources such as OWASP, CVE, NVD etc. and apply recommended patching to Product and or supporting systems as specified in integrated solution.