REGULATORY COMPLIANCE ATTACHMENT

Capitalized terms not otherwise defined herein will have the meanings ascribed to such terms in the Agreement.

1. COMPLIANCE WITH LAWS AND INTEGRITY

A. Supplier will comply with all laws, orders, rules, regulations and ordinances and Honeywell's Supplier Code of Business Conduct ("**Code**") in performing this Agreement. A copy of the Code may be obtained at http://hwll.co/CodeOfConduct. Supplier agrees to abide by the Code and maintain an integrity and compliance program that encompasses at a minimum the standards of business conduct set forth in the Code and that effectively prevents and corrects ethical violations and maintains compliance with laws. Supplier and its employees, agents, representatives and subcontractors have not made or received, and will not make or receive, directly or indirectly, any payments, loans, gifts, favors or other special consideration or form of compensation (a) to or from Honeywell, to its employees, agents or representatives, other than payments set forth in this Agreement or other written contractual agreement between Supplier and Honeywell; or (b) to or from any third party for the purpose of influencing the performance by Supplier or Honeywell of its respective duties hereunder. Supplier warrants and represents it has and will comply with the U.S. Foreign Corrupt Practices Act ("**FCPA**"), UK Bribery Act, EU and similar anti-bribery legislation or requirements. A breach of this provision will be deemed a material breach of this Agreement and grounds for termination of this Agreement.

B. Supplier acknowledges that in the event of Supplier's breach of its obligations, warranties and representations under this section, Honeywell may suffer damage to its reputation and loss of business which is incapable of accurate estimation.

C. Supplier will indemnify and hold harmless Honeywell from and against any and all loss, cost, expense (including reasonable attorney and professional fees), claims, damage, or liability arising out of or resulting from or occurring in connection with Supplier's breach of this Section.

2. U.S. GOVERNMENT COMPLIANCE

To the extent this Agreement (i) is in furtherance of a United States Government contract or subcontract that is subject to the U.S. Federal Acquisition Regulation (FAR) and/or other agency supplements, it incorporates by reference the Supplemental Provisions Under Fixed Price U.S. Government Contracts for Commercial Items (commercial products and services), or (ii) is funded or otherwise the subject of a United States Government Grant, it incorporates by reference the Supplemental Provisions Under U.S. Government Grants, both sets of Supplemental Provisions are accessible at Supplier Code of Business Conduct | Honeywell.

To the extent employment activities of Supplier occur in the United States and if otherwise applicable, this contractor and subcontractor will abide by the requirements of United States Federal Law, aligned with ensuring compliance with anti-discrimination laws.

3. NON-MILITARY END USER AND END USE CERTIFICATION (MEU RULE)

In order to satisfy U.S. export control laws, the Supplier confirms that it is not an entity that meets the definition of a military end user in China (including, Hong Kong and Macau), Russia, Belarus, Myanmar/Burma, Venezuela, or Cambodia ("**Military End User**") or sells items that support or contribute to a Military End Use by a Military End User. Military End User includes any entity that is part of the national armed services (army, navy, marine, air force, or coast guard), as well as the national guard and national police, government intelligence or reconnaissance organizations, or any person or entity whose actions or functions are intended to support "military end uses." "**Military End Uses**" includes use of an item to support or contribute to the operation, installation, maintenance, repair, overhaul, refurbishing, development, or production of military items. In addition, the Supplier will not divert or in any way utilize or sell products, materials, or technology/technical data/specifications supplied by or on behalf of Honeywell to Supplier under or in connection with the Agreement to/for any entity which is a Military End User or for Military End Uses by a Military End User. Supplier will immediately notify Honeywell and cease all activities associated with the transaction in question if it knows or has a reasonable suspicion that such products, materials, technical data, plans, or specifications may be exported, reexported, or transferred to a Military End User or in support of a Military End Use by a Military End User. Supplier's failure to comply with this provision will be deemed a material breach of the Agreement.

Notwithstanding anything to the contrary in the Agreement, Honeywell may take any and all actions required to ensure full compliance with applicable export control laws without Honeywell incurring any liability.

4. SANCTIONS COMPLIANCE

Supplier, individually and on behalf of its Affiliates, represents, warrants, and agrees that:

A. Supplier is not a "**Sanctioned Person**," meaning any individual or entity: (1) named on a governmental denied party or restricted list, including but not limited to: the Office of Foreign Assets Control ("**OFAC**") list of Specially Designated Nationals and Blocked Persons ("**SDN List**"), the OFAC Sectoral Sanctions Identifications List ("**SSI List**"), or any other sanctions list administered by the United States, the European Union and its Member States, the United Kingdom, Switzerland, Canada, Australia, or the United Nations ("**Sanctions Laws**"); (2) organized under the laws of, ordinarily resident in, or physically located in a jurisdiction subject to comprehensive sanctions administered by OFAC (currently Cuba, Iran, North Korea, Syria, and the Crimea, Donetsk People's Republic, and Luhansk People's Republic regions) ("**Sanctioned Jurisdictions**"); and/or (3) owned or controlled, directly or indirectly, 50% or more in the aggregate by one or more of any of the foregoing; and/or (4) organized under the laws of, ordinarily resident in, or located in an unauthorized jurisdiction, including Russia; Belarus; and the Zaporizhzhia and Kherson regions ("**Unauthorized Jurisdictions**").

B. Relating to this Agreement, Supplier is in compliance with and will continue to comply with all Sanctions Laws. Supplier will not involve any Sanctioned Persons, Sanctioned Jurisdictions, or Unauthorized Jurisdictions in any capacity, directly or indirectly, in any part of this transaction and performance under this transaction. Supplier will not take any action that would cause Honeywell to be in violation of Sanctions Laws.

C. Supplier will not source any components, technology, software, or data for utilization in Honeywell products or services: (a) from any Sanctioned Persons, Sanctioned Jurisdictions, or Unauthorized Jurisdictions (b) in contravention of any Sanctions Laws. Supplier will not sell, export, re-export, divert, use, or otherwise transfer any Honeywell products, technology, software, or proprietary information: (i) to or for any Sanctioned Persons or to or involving Sanctioned or Unauthorized Jurisdictions; or (ii) for purposes prohibited by any Sanctions Laws.

D. Supplier is responsible for conducting on-going screening and monitoring and ensuring all involved sub-suppliers and third parties are not Sanctioned Persons. Supplier is responsible for flowing down the obligations of this clause to all other involved sub-suppliers and third parties, as applicable.

E. Supplier's failure to comply with this provision will be deemed a material breach of this Agreement, and Supplier will notify Honeywell immediately if it violates, or reasonably believes that it will violate, any terms of this provision. Supplier agrees that Honeywell may take any and all actions required to ensure full compliance with all Sanctions Laws without Honeywell incurring any liability.

5. SOCIAL AND ENVIRONMENTAL GOVERNANCE

A. General. Supplier will comply with all applicable national, EU, state/provincial and local environmental, health and safety laws, regulations or directives.

B. Management System. Supplier must have a management system dedicated to compliance with applicable environmental, health and safety laws and regulations to ensure a safe working environment for their employees and responsible care of materials to prevent a negative impact on the environment (for example: ISO14001:2015/OHAS 18001:2007).

C. REACH. Upon request, in form and substance satisfactory to enable Honeywell to meet its compliance obligations with regard to Regulation (EC) No 1907/2006 ("**REACH**"), Supplier will provide Honeywell with complete information regarding the chemical composition (substances, preparations, mixtures, alloys or goods) of any Deliverables supplied under this Agreement, including all safety information required under REACH and information regarding the registration or pre-registration status of any Deliverables pursuant to REACH promptly but no later than 45 days of receiving such request. Supplier agrees that it will include any Honeywell "Identified Use" in its REACH registrations or applications for Authorization, unless Supplier notifies Honeywell that it rejects the Identified Use in order to protect human health or the environment and

specifies the reason for the rejection. In this case Honeywell will have the right to terminate this Agreement, without incurring any damages.

D. RoHS Directives. Absent Honeywell's prior written consent, no Deliverables will contain any of the substances identified in Article 4.1 of the European Parliament Directive (2011/65/EU collectively, the "**RoHS Directives**") (as such RoHS Directives are updated from time to time) or similar applicable laws or regulations, restricting the use of hazardous materials in other jurisdictions.

E. Montreal Protocol. Deliverables will not include any of the restricted chemicals set forth in the Montreal Protocol on ozone-depleting substances.

F. Proposition 65. Supplier will comply with its obligations under the Safe Drinking Water and Toxic Enforcement Act of 1986 of the State of California ("**Proposition 65**"). If the Deliverables contain any Proposition 65 listed chemicals, the Deliverables will be delivered with the warning labeling in full compliance with Proposition 65. If such chemicals are within safe harbor levels not requiring warning labeling under Proposition 65, Honeywell may request Supplier to provide certification, test protocol and test results evidencing that warning labeling is not required.

G. WEEE Directive. Supplier will be responsible for all costs and liabilities for or relating to the recycling of Deliverables pursuant the most current version of European Parliament Directive 2012/19/EU (the "**WEEE Directive**") as the WEEE Directive is updated from time to time and as any such Directive is implemented in any country.

H. Toxic Substances. Supplier will avoid use of materials of concern in the Deliverables provided to Honeywell, including but not limited to persistent, bioaccumulative toxic (PBT) substances, persistent organic pollutants (POPs) (e.g. PCBs, mercury, certain insecticides-DDT, Chlordane etc.), carcinogens (known or suspected), mutagens, radioactive materials, reproductive toxins (known or suspected), beryllium, hexavalent, chromium, asbestos or other respirable fibers, ozone depleting substances, brominated flame retardants or nanoparticles. Supplier will pro-actively inform Honeywell of any above listed substances content in any Deliverables supplied under this Agreement. If applicable, Supplier will be responsible for all costs and liabilities for or relating to the disposal and/or recycling of materials, waste and products.

I. Conflict Minerals Compliance. In accordance with applicable "Conflict Minerals" laws, Honeywell must determine whether its products contain tin, tantalum, tungsten or gold ("**3TG**") originating in the Democratic Republic of the Congo and adjoining countries ("**Conflict Minerals**"). To the extent Supplier supplies direct materials containing 3TG to Honeywell under this Agreement, Supplier commits to have a supply chain process to ensure and document a reasonable inquiry into the country of origin of the 3TG minerals incorporated into products it supplies to Honeywell. If requested, Supplier will promptly provide information or representations that Honeywell reasonably believes are required to meet its conflict minerals compliance obligations.

J. Per- and Polyfluorinated Substances (PFAS) Disclosure. Supplier has an affirmative duty to disclose to Honeywell, in writing, any products, components, materials or other items (collectively, "**Items**") it provides under this Agreement that contain Per- and Polyfluorinated Substances ("**PFAS**"), as that term is used in regulations requiring the reporting of such substances, including those issued by the US Environmental Protection Agency, either in or on the Items or used in the manufacture of the Items ("**PFAS Items**"). This is a continuing duty to disclose from the Effective Date of this Agreement through fulfillment of the last order hereunder, even if Supplier begins providing the PFAS Items after commencement of this Agreement. Further, Supplier represents and warrants that it has a process, or will implement one within 6 months of the Effective Date, for reasonably ascertaining whether and where PFAS Items may be entering Supplier 's supply chain. Following any such disclosures, the Parties will cooperatively work to ascertain the specific chemicals contained in any PFAS Items, and how to mitigate or eliminate them.

6. IMPORT AND EXPORT COMPLIANCE

A. Import. In the event government authorities declare or otherwise impose countervailing duties, antidumping duties, or retaliatory duties on the goods imported under this Agreement, Honeywell reserves the right to terminate this Agreement in accordance with the Termination provisions.

B. Export. Supplier will comply with all export laws and regulations of all countries involved in transactions associated with this Agreement.

In this Import and Export Compliance clause, "**Technical Information**" means any information which is necessary for one or more of the following activities: design, development, production, manufacture, assembly, installation, operation, repair, overhaul, testing, refurbishing, maintaining, or modifying a commodity (i.e., hardware, material) or software.

If the receiving Party receives hardware, Technical Information, manufacturing drawings, specifications, software or similar type items from the disclosing Party, it is the responsibility of the receiving Party to ensure compliance with all U.S. export laws and regulations, as well as all applicable local export laws and regulations if the receiving Party is located outside the U.S., in the performance under this Agreement. These laws include, but are not limited to, (a) Section 38 of the Arms Export Control Act as enumerated in 22 CFR Parts 120-130, the International Traffic in Arms Regulations ("**ITAR**"), and (b) Export Control Reform Act of 2018, as amended in 15 CFR Parts 730-774 of the Export Administration Regulations ("**EAR**"), and all applicable local export laws and regulations if the receiving Party is located outside the U.S. To the extent items are covered in the United States Munitions List (USML) and those items will be delivered to the U.S. GovernmentDFAR 252.225-7007 Prohibition on Acquisition of United States Munitions from Communist Chinese Military Companies (Sep 2006) will apply.

No hardware, Technical Information, manufacturing drawings, specifications, software or similar type items whose export is controlled by the U.S. Department of State or the U.S. Department of Commerce will be transferred, disclosed or exported to "**Foreign Persons**," not otherwise authorized, as defined in the above-stated laws and regulations, without specifically obtaining approvals from the U.S. Department of State's Office of Defense Trade Controls or from the U.S. Department of Commerce's Bureau of Industry and Security, as required.

If the receiving Party intends to transfer, disclose or export any of the disclosing Party Technical Information, manufacturing drawings, specifications, software or similar type items to any Foreign Persons not already authorized, prior written authorization of the disclosing Party must be obtained prior to the receiving Party obtaining U.S. Government licenses or other approvals as stated above. The receiving Party agrees to abide by all limitations and provisos and/or riders and conditions listed on any licenses or other approvals issued by the U.S. Department of State or the U.S. Department of Commerce.

7. SUPPLY CHAIN SECURITY

To the extent Supplier provides Goods that are shipped over U.S. borders, this section will apply.

Supplier represents and warrants that it (and its subcontractors) meet one of the criteria below and will accordingly continue to comply as follows:

If Supplier is US Customs – Trade Partnership Against Terrorism ("**C-TPAT**") certified, then Supplier will:

A. Advise Honeywell of its certification status and make its company visible for search in the C-TPAT Portal,

B. Authorize C-TPAT certification monitoring by Honeywell, and

C. Complete an annual survey attesting to C-TPAT program compliance.

If Supplier is certified by another World Customs Organization ("**WCO**") sanctioned supply chain security program (Authorized Economic Operator – AEO, Partners in Protection – PIP, etc.), then Supplier will:

A. Provide its certification number,

B. Complete an annual survey attesting to WCO compliance, and

C. Upon Honeywell's request, provide Honeywell with sufficient evidence of the WCO-sanctioned supply chain security program compliance.

If Supplier is neither C-TPAT certified, nor certified by an AEO, PIP, or other WCO-sanctioned program, then Supplier will:

A. Adhere to the security criteria for Supplier's applicable C-TPAT category (e.g., Importer, Foreign Manufacturer, etc.), and

B. Upon Honeywell's request, complete an annual survey attesting to its compliance with a WCO-sanctioned program.

8. DATA PRIVACY

A. "**Applicable Data Privacy Laws**" means applicable data protection, privacy, breach notification, or data security laws or regulations.

"**Business Contact Details**" means business contact details relating to an individual in a Party's business, such as first name, last name, initials, email address, job title or place of work, that are needed by the other Party for the purposes of managing the relationship between the Parties.

"**Personal Data**" means any information relating to an identified or identifiable natural person as defined under Applicable Data Privacy Laws.

The terms "**Service Provider**" or "**Contractor**" will have the meaning defined in the California Consumer Privacy Act (CCPA) as amended or analogous definitions in Applicable Data Privacy Laws.

B. Each Party may process the Business Contact Details or additional categories of Personal Data of the other in connection with this Agreement as an independent Data Controller (as that term or similar variants may otherwise by defined under Applicable Data Privacy Laws) to the extent necessary to perform their obligations hereunder. If the Parties transfer Personal Data from the European Economic Area (EEA), UK, Switzerland or any other jurisdiction that restricts the cross-border transfer of Personal Data or requires a data transfer mechanism for data transfers to locations outside of that jurisdiction, each Party agrees to be bound by the terms of the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (including the provisions in Module 1) and the UK's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses made under s119A(i) of the UK's Data Protection Act 2018 ("**Controller SCCs**") in its capacity as "data exporter" or "data importer," as applicable, and as those terms are defined therein. For jurisdictions outside of the EEA, all references to "GDPR" in the Controller SCCs will be deemed to refer to the Applicable Data Privacy Law. The Controller SCCs will be deemed to have been signed by each Party and are hereby incorporated by reference into the Agreement in their entirety as if set out in full as an annex to this Agreement. The Parties acknowledge that the information required to be provided in the appendices to the Controller SCCs is set out in the "Controller to Controller Transfers" document published at https://www.honeywell.com/us/en/company/data-privacy. If there is a conflict between this Agreement and the SCCs, the Controller SCCs will prevail. Where there is a change in the law that requires that the Controller SCCs be amended or replaced, such legally required changes will be deemed to have been made automatically without further action by the Parties.

C. To the extent that the provision of the Products, Services, Equipment, Works and/or Deliverables requires Supplier to process Personal Data as a processor, Service Provider or Contractor on behalf of Honeywell (or Honeywell's customer) as a controller or "Business," the Honeywell Data Processing Exhibit for Suppliers added to this attachment will apply to the processing.

9. SECURITY TERMS AND CONDITIONS AND AI SYSTEMS

A. Supplier will comply with the Honeywell's Artificial Intelligence (AI) Supplier Terms and Conditions Exhibit added to this attachment, if any.

B. Security Terms and Conditions. Supplier will comply with Honeywell's Security Terms and Conditions for Suppliers added to this attachment.

HONEYWELL'S DATA PROCESSING EXHIBIT FOR SUPPLIERS

This Exhibit applies where Honeywell is Controller and Supplier is a Processor. For the purposes of the Data Privacy Section of this attachment**,** the following will apply to Personal Data processed on Honeywell's behalf:

This Honeywell Data Processing Exhibit for Suppliers ("**Data Processing Exhibit**") forms part of the Agreement between Honeywell and Supplier and applies to the extent Supplier processes Personal Data on behalf of Honeywell (or Honeywell's customer) in the course of providing the Products, Services, Equipment, Works and/or Deliverables under the Agreement. All capitalized terms not defined herein will have the meaning set forth in the Agreement. In event of conflict between this Data Processing Exhibit and the Agreement, this Data Processing Exhibit will control with respect to its subject matter.

1. DEFINITIONS

"**Agreement**" means the written or electronic agreement between Honeywell and Supplier for the provision of the Services or the sale of Products, Equipment, Works and/or Deliverables to Honeywell.

"**Applicable Privacy Laws**" means applicable data protection, privacy, breach notification, or data security laws or regulations.

"**Controller**" means a natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data. The Controller may be Honeywell or Honeywell's customer.

"**Honeywell Personal Data**" means Personal Data Processed by Supplier on behalf of Honeywell in connection with Supplier's performance of its obligations under the Agreement.

"**Security Incident**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised access, disclosure, or use of Honeywell Personal Data while Processed by Supplier and/or its Subprocessors under this Data Processing Exhibit.

"**Sell**" or "**sale**" means selling, renting, releasing, disclosing, disseminating, making available, transferring or otherwise communicating orally, in writing, or by electronic or other means, a consumer's Personal Data by one business to another business or a third party for monetary or non-monetary consideration. Sale does not include the sharing or transfer of Personal Data by Honeywell to Supplier for the provision of the Services or the sale of Products, Equipment, Works and/or Deliverables on behalf of Honeywell under the Agreement.

"**Subprocessor**" means any Processor engaged by Supplier for the provision of the Services or the sale of Products, Equipment, Works and/or Deliverables including Supplier's affiliates and service providers that process Honeywell Personal Data pursuant to the Agreement.

The terms "**Data Subject,**" "**Personal Data,**" "**Processor,**" and "**Processing**" will have the meaning defined in the GDPR or analogous definitions in Applicable Privacy Laws.

2. PROCESSING

A. Role of the Parties. As between Supplier and Honeywell, Supplier will Process Honeywell Personal Data under the Agreement as a Processor acting on behalf of Honeywell as the Controller (except where Honeywell acts as a Processor in which case Supplier is a Subprocessor).

B. Instructions. Supplier will Process Honeywell Personal Data in accordance with Honeywell's documented instructions unless required to so do by applicable law to which Supplier is subject. Supplier is not responsible for determining whether Honeywell's instructions are compliant with applicable law. However, if Supplier is of the opinion that Honeywell's instruction infringes Applicable Privacy Laws, it will inform Honeywell of that legal requirement unless applicable law prohibits such notification. Any additional or alternate instructions must be agreed between the Parties in writing, including the costs (if any) associated with complying with such instructions. Upon notice in writing, Honeywell may terminate the Agreement if Supplier does not comply with Honeywell's lawful instructions that are within the scope of the Agreement to the extent such instructions are necessary to enable Honeywell to comply with Applicable Privacy Laws. Supplier will refund to Honeywell any unused prepaid fees or waive any termination fees or minimum commitment if Honeywell terminates the Agreement on these grounds.

C. Purpose limitation. Supplier will only process Honeywell Personal Data as permitted under the Agreement and Applicable Privacy Laws. Supplier is prohibited from selling, sharing (as may be defined under Applicable Data Privacy Laws), combining, retaining, using or disclosing any Honeywell Personal Data to any third party for the commercial benefit of Supplier or any third party, or to otherwise Process the Honeywell Personal Data outside of the direct business relationship between the Parties. Supplier certifies that it understands and will comply with all restrictions placed on its Processing of the Honeywell Personal Data.

D. Processing Details. The subject matter, duration of Processing, nature and purpose of Processing, the type of Honeywell Personal Data and categories of Data Subjects are specified in this Data Processing Exhibit.

3. SUBPROCESSORS

A. Authorization to use Subprocessors. Honeywell authorizes Supplier to use Subprocessors from the agreed list in the Subprocessor Annex to Process Honeywell Personal Data provided Supplier contractually requires Subprocessors to abide by terms no less restrictive than this Data Processing Exhibit. Supplier will be liable to Honeywell for the performance of its Subprocessor's data protection obligations under the Agreement.

B. Notification of intended changes. Supplier will notify Honeywell of any intended changes to its Subprocessors and will give Honeywell thirty (30) days to object after receipt of the notification. If Honeywell legitimately objects to a Subprocessor on reasonable data protection grounds and the Parties do not resolve the matter within one month following notification of the same to Honeywell, Honeywell may suspend or terminate the Agreement without penalty on written notice.

4. SECURITY

A. Security Measures by Supplier. To ensure the security of Honeywell's Personal Data, Supplier will implement the technical and organizational measures specified in the *Honeywell Security Terms and Conditions for Suppliers Attachment* attached to the Agreement and incorporated herein by reference. Supplier's security controls will comply with Applicable Privacy Laws and take into account industry standards, the nature of the Honeywell Personal Data, and the risks represented by Supplier's Processing of the Honeywell Personal Data by virtue of the physical, logical, or natural environment in which the Honeywell Personal Data is stored or Processed. Supplier will apply specific restrictions and additional safeguards if it Processes sensitive personal data (as defined under Applicable Privacy Laws) on behalf of Honeywell.

B. Confidentiality. Supplier will ensure that only authorized personnel who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality may Process Honeywell Personal Data for the purposes of performing the Agreement.

5. **SECURITY INCIDENT**

A. Notification. Supplier will notify Honeywell without undue delay after becoming aware of a Security Incident. Supplier will investigate the Security Incident and provide Honeywell with relevant information as required under Applicable Privacy Laws. Such information must at least include a description of the Security Incident including where possible, the nature of the Honeywell Personal Data concerned, the categories and approximated number of the Data Subjects and Personal Data records concerned, the likely consequences of the Security Incident and the measures taken or proposed by Supplier to remediate the Security Incident and mitigate its effects.

B. Assistance. Supplier will cooperate with Honeywell in notifying the Security Incident to a supervisory authority, customer of Honeywell, and/or affected Data Subjects and to carry out any recovery or other action necessary to remedy the Security Incident as required under Applicable Privacy Laws. At Honeywell's option, Supplier will either: (a) provide, at Supplier's own cost and expense and pursuant to Honeywell's direction, notice to the Data Subjects affected by the Security Incident in a manner that is consistent with Applicable Privacy Laws and, to the extent deemed appropriate by Honeywell under the circumstances, at least one (1) year of credit-monitoring and identity theft insurance services; or (b) reimburse Honeywell for all costs incurred to provide the same. Supplier will respond promptly and fully cooperate to all inquiries from Honeywell, any supervisory authority or government authority regarding the

Security Incident. Upon request and periodically as additional information becomes available, Supplier will, without undue delay, provide Honeywell with updates on the status of the Security Incident until the matter has been fully addressed and remediated.

C. Third party communications. Prior to Supplier's release, publication, transmission, or communication to any third party (including any supervisory authority, the media, or any affected Data Subject) relating to a Security Incident (collectively, "**Breach Communications**"), Supplier must first obtain prior written approval from Honeywell to the extent that (a) Honeywell or any of its Affiliates are specifically named or referenced in such Breach Communications; (b) Honeywell Personal Data or Honeywell systems are affected by the Security Incident; (c) the Breach Communications are directed at Honeywell's or its Affiliates' employees, suppliers, or customers; or (d) Honeywell may have certain independent legal, regulatory, or contractual obligations as a result of the Security Incident.

6. **DEMONSTRATING COMPLIANCE**

Upon Honeywell's written request and subject to obligations of confidentiality, Supplier will (and will ensure that its Subprocessors will) provide to Honeywell all information necessary to demonstrate its compliance with this Data Processing Exhibit. Honeywell (or an independent auditor mandated by Honeywell) may audit Supplier's compliance with such obligations at regular intervals or if there are indications of non-compliance with the terms of this Data Processing Exhibit ("**Audits**"). At Honeywell's request, upon reasonable notice, Supplier will also permit and contribute to onsite audits or inspections. In deciding on a review or Audit, Honeywell may consider any relevant certifications (such as SOC 2 Type II report) held by Supplier. Supplier will deal promptly and adequately with Audit inquiries from Honeywell. If Supplier, or any Subprocessor, is in breach of any of its obligations under the Agreement relating to Honeywell Personal Data, Honeywell may (without prejudice to any other rights or remedies it may have) suspend the transfer of Honeywell Personal Data to Supplier until the breach is remedied.

7. DATA TRANSFERS

A. Authorisation for Data Transfers. Honeywell hereby authorizes Supplier and its Subprocessors to transfer Honeywell Personal Data to locations outside of its country of origin for the performance of the Agreement provided that Supplier ensures such data transfers comply with Applicable Privacy Laws.

B. Data Export Restrictions. If Honeywell transfers Honeywell Personal Data from the European Economic Area, UK, Switzerland or from any other jurisdiction that restricts the cross-border transfer of Honeywell Personal Data to locations outside that jurisdiction, Honeywell will be bound by the Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 including the provisions in Modules 2 and 3, as applicable, and the UK's International Data Transfer Addendum to the EU Commission Standard Contractual Clauses made under s119 A(i) of the UK's Data Protection Act 2018 ("**Processor SCCs**") in the capacity of "data exporter," and Supplier in the capacity of "data importer" as those terms are defined therein. The Processor SCCs will be deemed to have been signed by each Party and are hereby incorporated by reference into the Agreement in their entirety as if set out in full as an annex to this Exhibit. The Parties acknowledge that the information required to be provided in the appendices to the Processor SCCs is set out below in the Description of Processing and Transfer Annex as a "description of the transfer" and "*Honeywell's Security Terms and Conditions for Suppliers Attachment*" set out in the Agreement as a "description of the technical organizational measures." If there is a conflict between the provisions of this Data Processing Exhibit or the Agreement and the Processor SCCs, the Processor SCCs will prevail.

8. **COOPERATION**

Supplier will promptly notify Honeywell of any request or complaint that it receives from a Data Subject, supervisory authority or any third party relating to the Processing of Honeywell Personal Data under the Agreement. Supplier will not respond to any request or complaint itself unless authorized to do so by Honeywell or as required by applicable law. Supplier will cooperate with Honeywell in fulfilling its obligations to respond to Data Subjects, conduct a privacy impact assessment or prior consultation with the supervisory authorities, provided that Honeywell reimburses Supplier for all reasonably incurred costs. If Supplier receives a Data Subject request relating to Honeywell Personal Data, Supplier will refer such Data Subject request to Honeywell within two (2) business days following receipt of the request.

9. **TERMINATION**

   Upon termination of the Agreement, Supplier will return, delete or anonymize all Honeywell Personal Data in accordance with the Agreement except to the extent Supplier is required by applicable law to retain Honeywell Personal Data in which case the terms of this Data Processing Exhibit will continue to apply to the retained Honeywell Personal Data.

10. **SURVIVAL**

    The undertakings in this Data Processing Exhibit will remain in force even after termination or expiration of the Agreement and/or the applicable Statements of Work for whatever reason.

11. **NOTICES**

    Notwithstanding anything to the contrary in the Agreement, all notices that Supplier is required to provide to Honeywell pursuant to this Data Processing Exhibit must sent by email with a read receipt to HoneywellPrivacy@Honeywell.com.

12. **AFFILIATES**

    This Data Processing Exhibit is entered into by Honeywell for and on behalf of itself and each of its Affiliates described in the Affiliates Annex to this Data Processing Exhibit.

SUBPROCESSOR ANNEX TO HONEYWELL'S DATA PROCESSING OBLIGATIONS FOR SUPPLIERS EXHIBIT

To support delivery of the Services to Honeywell under the Agreement, Supplier may engage and use third-party contractors to provide certain services on its behalf (each a "Subprocessor"). Supplier will, upon written request, provide a list of Subprocessor(s) containing the purpose of the sub-processing, the location of the Subprocessor and the data transfer mechanism.

AFFILIATES ANNEX TO HONEYWELL'S DATA PROCESSING OBLIGATIONS FOR SUPPLIERS EXHIBIT

This Data Processing Exhibit is entered into by Honeywell for and on behalf of itself and its Affiliates identified on the list available at https://www.honeywell.com/us/en/honeywell-affiliates as updated from time to time.

DESCRIPTION OF THE PROCESSING AND TRANSFER ANNEX (MODULE 2: CONTROLLER TO PROCESSOR OR MODULE 3: PROCESSOR TO PROCESSOR)

A. LIST OF THE PARTIES	
Controller/Data Exporter:	Name: Honeywell International Inc., its Affiliates, and subsidiaries Address: 855 S. Mint St., Charlotte, NC 28202, USA Contact: Chief Privacy Officer Email: HoneywellPrivacy@honeywell.com
Processor/Data Importer	The full name, address and contact details for the Party is set out in the Agreement.
B. DETAILS OF PROCESSING/TRANSFER	
CATEGORIES OF DATA SUBJECTS	Dependent on the Data Exporter's use of the Data Importer's Services as per the Agreement, the Data Exporter may elect to include Personal Data from any of the following types of data subjects: • Employees, contractors, temporary workers, directors, company officers, shareholders and agents (current, former, prospective) of data exporter • Beneficiaries, dependents, and relatives of the data subject • Channel Partners, distributors, sales partners, and business partners • Advisors, trainers, consultants, service providers and other third parties • Users (e.g., customers) and end users of data exporter's Product and Services • Any other data subject as described in the Agreement.

CATEGORIES OF PERSONAL DATA	Dependent on the Data Exporter's use of the Data Importer's Services as per the Agreement, the Data Exporter may elect to include Personal Data from any of the following categories of Personal Data: • Basic personal data (for example first name, last name, initials, email address, job title, country of residence, mobile phone number) • HR and recruitment data (for example basic employment data, education data, demographic data, employment status, job and position data, worked hours, holidays, assessments, performance appraisals, salary, benefits, work permit details, availability, terms of employment, tax details, payment details, insurance details, travel information and recruitment information such as curriculum vitae, employment history, education history details) • Authentication data (for example username, password, security question, audit trail) • Unique identification numbers and signatures (for example IP addresses, unique identifiers in tracking cookies or similar technology) • Citizenship and residency information (for example nationality, citizenship, naturalization status, immigration status, passport data, details of residency or work permit) • Biometric Information (for example facial recognition, fingerprints, and iris scans) • Commercial Information (for example history of purchases, special offers and payment history) • Support Services (for example personal data collected through the provision of support services online or interactive communications) • IT systems and operational information (for example unique identifiers, voice, video and data recordings, tracking of information regarding the patterns of hardware, software, device and internet usage, IP addresses, domains, apps installed, browsing and support logs, incidental access of the content of email communications and data relating to the sending, routing and delivery of emails whilst providing support services) • Location data (for example, mobile device ID, geo-location network data, location data derived from use of wi-fi access points) • Device identification (for example UUID, IMEI-number, SIM card number, MAC address); • Training and development (for example trainee data, training history, individual development plans, trainer information and training schedules) • Photos, video and audio (for example webcam or voice recordings)
SPECIAL CATEGORIES OF DATA (IF APPLICABLE)	Dependent on the Data Exporter's use of the Data Importer's Services, the Data Exporter may elect to include Personal Data from any of the following special categories of Personal Data which is in the scope of the Services: Racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person's sex life or sexual orientation, gender orientation, data relating to criminal convictions or offences or precise geolocation data or any other type of personal data provided under the Agreement that is considered sensitive under Applicable Privacy Laws.
FREQUENCY OF THE TRANSFER	The data transfers under the Agreement will take place on a continuous basis.

NATURE OF THE PROCESSING	Data Importer and its Subprocessors are providing Services or fulfilling contractual obligations to the Data Exporter as described in the Agreement. These Services may include the processing of Personal Data by Data Importer and/or its Subprocessors.
PURPOSE OF PROCESSING/ TRANSFER	Dependent on the Data Exporter's use of the Data Importer's Services as per the Agreement, the Data Exporter's Personal Data is processed, and transfer is made for the following purposes: • Relationship management: facilitating communication with customers, employees and users for the services performed under the Agreement. • HR and recruitment: the processing of applicant and employee personal data for the purposes of administering, organizing, and managing the applicant and employment relationship. • Service management: the provision and deployment of products and related services, consultancy, data migration, installation of systems and software, provision of support and maintenance services, training, channel and/or supplier administration and support. • Channel: administration and management of channel partners, distributors and/or sales partners. • Marketing: administration and management of marketing databases for direct marketing purposes, conduct of marketing activities/campaigns. • Management of electronic identity and communication: identity management, security management, confidentiality of data exporter and data exporter's customers and employees. • Operating and managing the IT and communications systems, managing product and service development, improving existing and developing new products and services, research and development, managing company assets, allocating company assets and resources, strategic planning, project management, business continuity. • Training: administration of learning managements systems, facilitation of onsite and online learning. • Research in any field including scientific and technical research. Any other scope and purpose as described in the Agreement.
RETENTION	The Data Exporter's Personal Data will be retained in accordance with the Agreement unless applicable law requires storage of the Personal Data for a longer period.
COMBINATION OF DATA	Personal Data received from the Data Exporter is combined with Personal Data collected by the Data Importer unless otherwise prohibited by the Agreement.

TRANSFER TO SUBPROCESSORS	The Data Importer may process and transfer Personal Data to Subprocessors in relation to the performance of the Agreement and in accordance with the following scope:
	• **Subject Matter**
	  ○ The subject matter of the processing under the Agreement is the Personal Data.
	• **Nature of the processing**
	  ○ Data importer and its Subprocessors are providing Services or fulfilling contractual obligations to the data exporter as described in the Agreement. These Services may include the processing of Personal Data by data importer and/or its Subprocessors.
	• **Duration**
	The duration of the processing under the Agreement is determined by the data exporter and as set forth in the Agreement.

LIST OF SUBPROCESSORS	The list of sub-processors is attached as the SUBPROCESSOR ANNEX TO HONEYWELL'S DATA PROCESSING OBLIGATIONS FOR SUPPLIERS EXHIBIT
C. COMPETENT SUPERVISORY AUTHORITY	
The competent supervisory authority will be the supervisory authority which has jurisdiction in relation to the activities of the Data Exporter as Controller under Applicable Privacy Laws or, where it is not established in applicable jurisdiction, where its representative has been established pursuant to applicable legal requirements or, if the Data Exporter does not have to appoint a representative, where the data subjects whose Personal Data are transferred are located.	
D. GOVERNING LAW AND CHOICE OF FORUM	
GOVERNING LAW	For the purposes of Clause 17 of the SCCs, the Parties select the law of Ireland.
CHOICE OF FORUM	For the purposes of Clause 18 of the SCCs, the Parties select the courts of Ireland.
E. OTHER	
Where the SCCs identify optional provisions (or provisions with multiple options) the following will apply:	For Clause 7 (Docking Clause), the optional provision will apply
	For Clause 9 (a), option 2 will apply. The parties will follow the process agreed in Section 3 (Subprocessing) of the Honeywell Data Processing Exhibit.
	For Clause 11(a) (Redress) – the optional provision will not apply

HONEYWELL SECURITY TERMS AND CONDITIONS FOR SUPPLIERS

Supplier will implement appropriate technical and organizational measures to ensure the confidentiality, integrity, authenticity, and availability of the data, assets, processes, systems, personnel, and sites used by Supplier in the performance of this Agreement. These measures will comply with good industry practices, including without limitation (i) ensuring that all employees with access to confidential information complete security awareness training that includes protection of such information; (ii) conducting legally permissible background screening and verification on all employment candidates who have access to Confidential Information pursuant local laws, regulations, ethics and contractual constraints; (iii) sanitizing all data storage media before redeployment or disposal such that data cannot be reconstructed; and (iv) notifying the respective Honeywell account focal and send an email message to CIRT@honeywell.com with the relevant incident for any incident involving Honeywell information. Supplier shall ensure that any subcontractors implement substantially similar measures and shall remain liable for the performance of such subcontractors.

Additional security terms and conditions will be required if the scope of the Agreement extends to the performance of Covered Services by Supplier (defined below). Prior to the performance of such Covered Services, the Parties agree to execute, or amend the Agreement to incorporate, the Honeywell Security Terms and Conditions for Suppliers applicable to the Covered Services contemplated by such amendment, statement of work, or purchase order. For purposes of this Agreement, “Covered Services” means any of the following: (i) receiving, accessing, interacting with, storing, transmitting, or otherwise processing Confidential Information of Honeywell or its customers; (ii) accessing, integrating with, connecting to, or administering the IT or OT systems of Honeywell or its customers; (iii) accessing facilities, equipment, or other physical resources of Honeywell or its customers; or (iv) supplying, developing, delivering, maintaining or supporting software, drivers, firmware, or products containing such code. The applicable Honeywell Security Terms and Conditions for Suppliers may be obtained by contacting CPSS@Honeywell.com or your Honeywell Sourcing point of contact.