HONEYWELL DATA PROCESSING AGREEMENT ("DPA") EXHIBIT

This DPA forms part of the Agreement and applies to the extent that Honeywell processes Company's Personal Data on behalf of the Customer in the course of providing the Services. The DPA does not apply where Honeywell is the Controller. All capitalized terms not defined herein shall have the meaning set forth in the Agreement. In event of conflict between this DPA and the Agreement, this DPA shall control with respect to its subject matter.

1. Definitions

"**Agreement**" means the written or electronic agreement between Company and Honeywell for the provision of the Services to Company.

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

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

"**Subprocessor**" means any Processor engaged by Honeywell for the provision of the Services including Honeywell affiliates and service providers.

Regardless of Applicable Privacy Laws, the terms "**Controller**", "**Data Subject**", "**Personal Data**", "**Processor**" and "**Processing**" will have the meaning defined in the General Data Protection Regulation EU 2016/679 ("**GDPR**") or analogous definitions in Applicable Privacy Laws.

2. Processing

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

2.2. Instructions. Honeywell will Process Company Personal Data in accordance with Company's documented instructions unless required to so do by applicable law to which Honeywell is subject. Company agrees that the Agreement and any subsequent statements of work are its complete and final instructions to Honeywell in relation to the Processing of Company Personal Data. Any additional or alternate instructions must be agreed between the Parties in writing, including the costs (if any) associated with complying with such instructions. Honeywell will inform Company if it is of the opinion that a Company instruction infringes Applicable Privacy Laws unless applicable law prohibits such notification on important grounds of public interest.

2.3. Purpose limitation. Honeywell will only process Company Personal Data as permitted under the Agreement and Applicable Privacy Laws. Honeywell will not sell (as the term is defined under Applicable Privacy Laws) any Company Personal Data to any third party.

2.4. Processing Details. The subject matter, duration of Processing, nature and purpose of Processing, the type of Company Personal Data and categories of Data Subjects are specified in Annex 1 to this DPA.

2.5. Compliance with Laws. Company warrants that its Processing of Company Personal Data complies with all Applicable Privacy Laws and any processing instructions it issues to Honeywell under the Agreement.

3. Subprocessors

3.1. Authorisation to use Subprocessors. Honeywell engages Subprocessors to provide certain services under the Agreement on its behalf. Company authorizes Honeywell to use Subprocessors located in any jurisdiction to Process Company Personal Data provided Honeywell contractually requires Subprocessors to abide by terms no less restrictive than this DPA. Honeywell will be liable to the Company for the performance of its Subprocessor's obligations under the Agreement.

3.2. Notification of intended changes. Honeywell will make available to Company a list of Subprocessors that it engages to support the provision of the Services upon written request.

Honeywell will notify Company of any changes to its Subprocessors ("Subprocessor Notices") and will give Company ten business days to object after receipt of the notification. If Company 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 terminate all or part of the Order Form impacted by the new Subprocessor without penalty on written notice.

3.3. Company is responsible for informing Honeywell of the email address to which Subprocessor Notices must be sent, by emailing HoneywellPrivacy@Honeywell.com with "Subprocessor Subscribe" in the subject line, giving details of the contact person, and the Service for which Subprocessor Notices are required. Company is also responsible for informing Honeywell of any changes to those details.

4. Security

4.1. Security Measures by Honeywell**.** Honeywell will use appropriate technical and organizational measures to protect Company Personal Data as required by Applicable Privacy Laws and will follow industry-standard security practices. A list of the technical and organizational measures implemented by Honeywell is attached to this Data Processing Exhibit as Annex 2. ("**Information Security Measures**"). Honeywell may update or modify the Information Security Measures provided that such updates and modifications do not result in a material degradation of the overall security of the Services provided under the Agreement.

4.2. Security Measures by Company. Company is solely responsible for determining whether the Information Security Measures meets its requirements and provides a level of security appropriate to the risks of Processing such Company Personal Data. Company acknowledges and agrees that the level of security provided by the Information Security Measures is appropriate to the risk inherent in the Processing by Honeywell on Company's behalf. Company is responsible for configuring the Services in a manner which enable Company to comply with Applicable Privacy Laws, including the implementation of appropriate technical and organisational measures.

4.3. Access and Confidentiality. Honeywell will ensure that only authorised personnel who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality may access Company Personal Data for the purposes of performing the Services under this Agreement.

4.4. Prohibited Data. Customer acknowledges and agrees that the Agreement may prohibit the submission of certain types of Personal Data (such as a PCI or health information) to the Services. Customer will not submit to the Services any Customer Personal Data which is regulated by COPPA, FERPA and HIPAA unless authorised to do so in writing by Honeywell.

5. **Security Incident.** Honeywell will notify Company without undue delay after becoming aware of a breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized access, disclosure or use of Company Personal Data while processed by Honeywell (each a "**Security Incident**") in relation to the Services under the Agreement to assist Company with its reporting or notice obligations under Applicable Privacy Laws. Honeywell will investigate the Security Incident and provide Company with relevant information about the Security Incident as required under Applicable Privacy Laws. Honeywell will use reasonable efforts to assist the Company in mitigating, where possible, the adverse effects of any Security Incident. Honeywell's notification to Company of a Security Incident will not be deemed an acknowledgement of fault or liability.

6. Compliance

6.1. Demonstrating compliance. Upon Company's written request and subject to obligations of confidentiality, Honeywell will provide to Company all information necessary, including by relevant certifications, to demonstrate its compliance with this DPA. Company (or an independent auditor mandated by Company) may audit Honeywell's compliance with such obligations once per year at the applicable facility or if there are indications of non-compliance

with the terms of this DPA ("**Audits**").

6.2. Audits. Audits will only be performed following Company's written request at least ninety (90) days prior to the proposed start date and Company providing a reasonably detailed audit plan describing the proposed scope, start date and duration. Before the commencement of an Audit, the Parties will agree on a final Audit plan. Audits will be conducted during Honeywell's regular business hours, subject to the published policies of the audited facility, and may not unreasonably interfere with business activities. The personnel conducting the Audit on behalf of Company or an independent auditor mandated by Company must enter into an appropriate written confidentiality agreement acceptable to Honeywell prior to conducting the Audit and will be accompanied by at least one member of Honeywell staff at all times. To preserve the security of the Honeywell organization and its companies, Honeywell reserves the right to not share information that could expose or compromise its security, privacy, employment policies or obligations to other customers or third parties or share confidential information. Records may not be copied or removed from Honeywell facilities. Company will generate and provide Honeywell with an audit report within three months after the Audit. All information obtained or generated in connection with an Audit, including audit reports, must be kept strictly confidential and may only be used for the purposes of confirming Honeywell's compliance with its obligations under this Data Processing Exhibit. Company will pay or reimburse Honeywell's reasonable costs for allowing for and contributing to Audits.

7. Data Transfers

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

7.2. Data Export Restrictions. If Honeywell transfers Company Personal Data from the European Economic Area ("EEA"), UK, Switzerland or from any other jurisdiction that restricts the cross-border transfer of Company Personal Data to locations outside that jurisdiction, Company shall 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 Honeywell 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 Agreement. The Parties acknowledge that the information required to be provided in the appendices to the Processor SCCs is set out in Annex 1 below as a "description of the transfer" and " Security Measures" as a "description of the technical organisational measures" in Annex 2. If there is a conflict between the provisions of this DPA or the Agreement and the SCCs, the SCCs will prevail.

8. **Cooperation.** Honeywell will cooperate with Company to respond to any requests, complaints or inquiries from data subjects, supervisory authorities, or other third parties, conduct a privacy impact assessment and prior consultation with supervisory authorities, provided that Company reimburse Honeywell for all reasonably incurred costs. If Honeywell receives a data subject request relating to Company Personal Data, Honeywell will refer such data subject request to Company. Honeywell will not respond to the data subject request unless required by applicable law**.**

9. **Termination.** Upon termination of the Agreement, at Company's option, Honeywell will return, delete or anonymize all Company Personal Data except to the extent Honeywell is required by applicable law to retain Company Personal Data or for compliance, audit or security purposes in which case the terms of this DPA will continue to apply to the retained Company Personal Data. The DPA and the Processor SCCs will terminate automatically upon the deletion or anonymization of the Company Personal Data processed under this DPA.

ANNEX 1
DESCRIPTION OF PROCESSING AND TRANSFER ACTIVITIES
(MODULE 2: CONTROLLER TO PROCESSOR)

A. LIST OF THE PARTIES	
Controller / Data Exporter:	The full name, address and contact details for the Party is set out in the Agreement.
Processor / Data Importer	The full name and address of the Honeywell entity specified in the Agreement. Contact: Chief Privacy Officer Email: HoneywellPrivacy@honeywell.com
B. DETAILS OF PROCESSING/TRANSFER	
CATEGORIES OF DATA SUBJECTS	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 types of data subjects: • Employees and staff (including applicants, contractors, temporary workers, trainees, interns, directors, company officers, shareholders, and agents) • Channel partners, distributors, sales partners, business partners and service providers • Customers and their staff (including applicants, contractors, temporary workers, trainees, interns, directors, company officers, shareholders, and agents) • Users of the Data Importer's Services (including end users of Customers and other third parties) • Any other data subject as described in the Agreement which is in the scope of the Services provided.
CATEGORIES OF PERSONAL DATA	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 categories of Personal Data: • Business contact information (such as name, email address, gender, job title, country of residence, mobile phone number and location) • Employment data (such as compensation, qualifications, attendance data, curriculum vitae, employment history, education history, work permit, citizenship, and residency information) • Unique identification numbers and signatures (such as government identifiers, cookie identifiers or driver's license number) • Biometric information (such as facial recognition, fingerprints, and iris scans) • Commercial Information (such as history of purchases, special offers and payment history) • Support Services (such as personal data collected through the provision of support services online or interactive communications) • Information related to data subject's use of IT assets (such as username, password, security question, IP address, login information, credentials, data relating to the sending, routing and delivery of emails whilst providing support services, and incidental access of the content of email communications etc.) • Profiling (such as behaviour observed based on unique identifiers, patterns of hardware, software, device and internet usage, IP addresses, domains, apps installed, browsing and support logs etc.) • Location data (such as geo-location, network data, location data derived from use of wi-fi access points) • Device identification (such as UUID, IMEI-number, SIM card number, MAC address); • Training and development (such as trainee data, training history, individual development plans, trainer information and training schedules) • Photos, video, voice, and audio (for example webcam or voice recordings) • Any further Personal Data contained in an application or IT system which is in scope of the Services provided.

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, or data relating to criminal convictions or offences).
FREQUENCY OF THE TRANSFER	Dependent on the Data Exporter's use of the Services, the Data Importer may host, remotely access, or otherwise transfer Personal Data on a one-off basis or on a continuous basis when providing the Services as described in the Agreement.
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, 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 • 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 that is specified above.
	• **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.

C. COMPETENT SUPERVISORY AUTHORITY	
The competent supervisory authority shall 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 agree that the courts of Ireland will have jurisdiction.
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.

ANNEX 2

INFORMATION SECURITY MEASURES

Honeywell is committed to protecting personal and customer information. This appendix describes Honeywell's security measures for safeguarding personal and customer information that is processed within Honeywell Enterprise infrastructure. Any additional safeguards are outlined in the statement of work or IT Security exhibit as agreed with respective customer.

Honeywell has implemented the described measures across the Honeywell Enterprise-Wide Network (HEWN), for the security of personal and customer data.

Categories	Practices
Audits and Third-Party Certification	**Compliance and Certifications** Maintain an enterprise-wide information security policy framework to safeguard the confidentiality, integrity, and availability of all information assets and ensure regulatory, operational and contractual requirements are fulfilled. The control framework is aligned to NIST SP 800-171 controls and DoDs Cybersecurity Maturity Model Certification (CMMC) practices and includes development and policies, standards and procedures for suitable and applicable implementation. Compliance with these established security controls sets the foundation for protecting all Honeywell assets and interconnected systems. **Right to Audit** Third-party audit requirements are negotiated and executed per contract terms and conditions. **Audit Finding Remediations** Remediates audit findings by raising an issue. Each issue is tracked through a governance process with a defined remediation plan and ownership assigned.
Governance, Risk, and Compliance	**Policies and Standards** Policies and standards are governed at a global level to comply with a myriad of requirements and cannot be changed without consideration and coordination. **Threat Intelligence** Threat intelligence process in place with constant evaluations of our adversaries to determine the most effective controls. **Risk Management** Risk assessments are handled by multiple functions in the enterprise. Each function identifies different sources of risk to Honeywell and applies a standardized prioritization. Risk mitigation plans are recorded and implemented through the risk management and compliance issue management processes. All the risks are entered into the Risk Register and assigned mitigation plans, which are tracked with the owner. **Compliance Assessments** Risk and Compliance teams operate continuously to test controls, identify issues, facilitate remediation, and report progress and issues to senior leadership, including detailed dashboards and regular CIO briefings. The types of assessments conducted differ by service, process and assets. There are annual standard assessments, pro-active deep-dive assessments, and risk analysis/assessments conducted on a periodic basis. **Security Exceptions** Robust security exception process in place to service the global organization to assist the efficient and appropriate reduction of risk in the short term (less than a year) when scenarios such as non-whitelisted software must be addressed and mitigated.
Access Control	**Authorization** Enforce authorization controls for remote and wireless access to the company network prior to allowing such connection. System access and privileges are limited based on the types of transactions and functions authorized users are permitted to execute. **Least Privileges** Access to resources are limited to those who have a specific need to access systems and data. User access is only approved for the minimal requirements or least privilege necessary for an individual to perform job responsibilities.

Categories	Practices
	Identification Secure login with unique identification and authentication for all users attempting to access company systems. **Authentication** Enforce multi-factor authentication for remote and admin access with mandates for complex passwords. **Account Management** Role-based access controls are firmly in place. Manage identification, authentication, and access rights for all users. Maintain segregation of duties through role-based access control across all functions to reduce the risk of malevolent activity without collusion. Reviews of active users are conducted at minimum on a quarterly basis to ensure only authorized individuals have access to information systems. **Account Lockout and Revocation** Limit unsuccessful information system access after consecutive invalid login attempts. Screens and terminals protected against unauthorized access, no matter where they may be located; office, home, travel, etc. Active Directory access contingent upon employment status, when there is a change in status in the HR system, access is automatically revoked.
Network Security	**Architecture** Defense in depth strategy is employed, including network hardening/patching, centralized log collection and correlation, and deny all/permit by exception firewall configuration in a three-tier demilitarized zone architecture. All Internet traffic is routed only through data center Internet gateways. **Boundary Protection** Boundary protection is through managed firewalls (e.g., Checkpoint, DMZ, content filtering using proxies, Cisco TrustSec used for policy enforcement). Network perimeter security through intrusion detection and prevention systems and state of the art firewalls. **Network Segmentation** Internal boundaries are managed through physical firewalls to segment Specific Use Networks (SUNs) from the enterprise network. **Software-Defined Wide Area Network (SD-WAN)** SD-WAN provides rapid isolation of network segments from bad actors during incident management.
Asset and Configuration Management	**Asset Lifecycle Management** Information asset inventory and protection processes are designed to protect information throughout the lifecycle including creation, use, processing, storage, transmission and destruction. **Asset Inventory** Maintain an inventory system with a centralized configuration management database (CMDB) repository in which configurations common across multiple systems within the enterprise are stored. **Device Hardening** Honeywell follows approved configuration baseline security standards. The standard defines the mandatory tools that is approved by the Standards Council including security stakeholders. All functions, ports, protocols and services are documented in the local system run book, and each entry identifies a business requirement that justifies the service. **Configuration Management** Maintain centralized configuration management repository in which configurations common across multiple systems within the enterprise are stored in a repository, versioned, and deployed. Baseline configuration settings for all IT products are documented in build books. **Change Management**

Categories	Practices
	All changes, including patches related to infrastructure and applications within the production environment, are managed in a controlled manner. Changes are logged, assessed, and authorized prior to implementation and reviewed against planned outcomes following implementation. **Asset Destruction** Information assets are securely destroyed when no longer required including but not limited to disk drives, hardcopy documents, USB devices, network devices, mobile devices, copiers and optical media.
System and Communications Protection	**Operational Policy** Control and monitor user workstations using a Windows Group Policy Object (GPO). Each time a user logs in, the device is scanned, and baseline operating system settings are applied. Changes to the workstation configurations are proposed and reviewed monthly. Approved changes are tracked in the inventory system. **Software Authorization and Prohibitions** Approved software is provisioned through an automated end-user interface. Honeywell uses a centralized desktop scanning and inventory application, which includes licensing and entitlement management. **Encryption** Maintain strong cryptography and security protocols to protect the confidentiality and integrity of data in transit. Honeywell requires network access to occur locally or through encrypted channels. **Email Protections** Deployed Domain-based Message Authentication, Reporting and Conformance (DMARC) on all email managed domains to address the email security risk represented by so-called email spoofing. With DMARC, external attackers cannot impersonate the Honeywell email domain, and this helps prevent spam, spoofing and phishing. **Session Termination** Employ a 15-minute idle timeout for any device except for industrial control systems. **Mobile Device Security** Commercial Mobile Device Management (MDM) solution in place. All mobile devices are encrypted, and password protected. This ensures any data residing on the mobile device will be protected. MDM solution within the approved device is used to control the environment and data.
System Development and Maintenance	**Application Development Security** Projects follow agile development and DevOps principles, as appropriate. Rigorous pursuit of secure coding principles in the development and coding of applications/software. **Maintenance** Systems are maintained on a monthly patch cycle. System software components such as applications, database management systems, and web server software undergo security patches and version upgrades as means of software maintenance. **System Flaws** Assured compliance with Honeywell security standards. Identify, report, and correct server flaws using automated reports and manual processes. Server flaws are addressed in an expeditious manner by system administration and management.
Security Operations	**Audit (Logging) and Accountability** Centralized Security Information and Event Management (SIEM) system (Splunk) collects audit information in a single location. Within Splunk, only authorized systems administrators (privileged users) are allowed to record, enable or disable audit events such as password changes, failed logins, failed transactions, privileged usage, and credential usage. **Antivirus Protections** Maintain automatic scanning mechanisms on assets commonly affected by malicious code. Antivirus updates for the engine and signatures must be downloaded and installed from a centralized management infrastructure or trusted source at a minimum daily.

Categories	Practices
	Cyber Threat Awareness Security Operations Center (SOC), Cyber Threat Intelligence group is dedicated to monitoring and responding to cyber threat intelligence shared in both open-source and closed-source information repositories. **Intrusion Detection and Prevention** Intrusion and prevention detection systems are configured to detect activity and provide alerts for the high-risk protocols attempting to traverse zones of trust, as defined by governance documents. **Monitor and Detect Anomalies and Events** Suspicious activity is detected automatically by one of the security tools (i.e., such as intrusion detection systems, anti-virus software, system audits logs) or manually reported by an end-user or privileged user. Event correlation and escalation capabilities are provided by the software. **Continuous Monitoring** Security Operation Center (SOC) monitors the environment 24/7 for attacks, indicators of attacks, or suspicious activity in many aspects of the environment (i.e., network access, system access, emails, internet browsers).
Product Security	**Secure Development Lifecycle** Dedicated Software and Systems Development Engineering, Product Cyber Security, Customer Support, Program/Project Management, and other appropriate support teams. **Application Development Security** Maintain measures to ensure all products 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, threat modelling, product security risk-based testing and remediation requirements. **Code Signing** A Secure Development Policy is in place mandating that all software and firmware must be signed. Where code signing is not feasible, other technologies that achieve equivalent integrity may be used. **Security Testing** Source code reviews and security testing of hardware or software are conducted to identify potential system flaws, with the goal of mitigating risk, protecting data, and maintaining intended systems functionality. Requirements of security testing may include confidentiality, integrity, authentication, availability, authorization, and nonrepudiation. Actual requirements tested depend on the context of the security implemented by the system. **Product Security Incident Response** Honeywell's Product Security Incident Response Team (PSIRT) minimizes customer risk associated with security vulnerabilities.
Data Protection	**Data Protection Program** Data Protection Program employed with a suite of tools covering classification, ownership identification, monitoring, detection and prevention. **GDPR Compliance** Global Data Privacy Policy requires employees to comply with Data Protection Laws with respect to the processing of Personal Data. **Data Privacy** Personnel engaged in data processing are under a written obligation of confidentiality and may not collect, process or use personal data without authorization. Mandates for personal data encryption in transit and at rest. **Data Integrity** Robust information protection capabilities for all laptops, remote sessions, mobile devices and backups are encrypted. Email encryption of external communication is available and file shares can be encrypted on request.

Categories	Practices
	Data Loss Prevention Control and monitor extrusion detection systems to enforce data security policies and prevent loss of intellectual property and other Highly Confidential information. **Data Retention** Retain backup and archived electronic copies of data in its controlled information systems for audit purposes. **Secure Document Exchange** Provide options for secure exchange documents with customers based on the sensitivity of the information. **Media Protection** Approved selection of media, including associated information contained on that media, requiring physical protection. Provide sufficient protection with physical access controls to the facility where the media is stored. **Media Sanitization** Approved methods to sanitize all data unless dictated differently by local laws or customer contractual obligations. **Removable Media** Restrict the use of portable storage devices by default and authorizes use of Honeywell-approved, encrypted removable media, by exception, which ensures a connection with the owner. **Data Termination** Upon written request, Honeywell will return, delete or anonymize customer data, with the exception of archives and required retention.
Physical and Environmental Security	**Physical Security Protections** Physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) are implemented to safeguard sensitive information and information systems. **Data Center Environmental Controls** Tier 3 global data centers meet relevant industry standards. Physical controls are tested regularly by management as well as periodically validated through audits and risk assessments. **Limit Physical Access** Physical access to facilities and data centers is restricted in order to protect hosted information, applications, systems, and infrastructure. Controlled access points limit physical access to IT assets. All external access points require approved security controls. Access to the site is controlled by an approved mechanical and electronic access control system. **Visitor Access Control** All visitors must provide a government issued ID to enter the facility and be issued and wear a temporary access badge. Identification badges are used, and visitors must be accompanied by an escort. Visitor access is subject to approval and is maintained in accordance with Honeywell retention policy. **Surveillance** Where necessary, security cameras and security guards are utilized to observe and enforce access controls, protection of Honeywell employees, and Honeywell property. **Intrusion Detection and Prevention** The audit trail of activities captured via CCTV or access control systems is retained for a minimum of thirty (30) days or as permitted by applicable law.
Personnel Security and Training	**Onboarding New Hires** Hiring procedures for new employees require the completion of a detailed application form as allowed by local law and appropriate for job roles: • Educational verification; • Previous employment verification;

Categories	Practices
	• Social Security Number, National Identifier or Personal Identity Code validation; • Drug screen; • Criminal history check. **Awareness and Training** Annual compliance training for employees to complete an online course and pass an assessment covering information security and data privacy. The security awareness program may also provide materials specific to certain job functions. **Personnel Termination** Terminations are initiated by the employee's supervisor. Cyber access is contingent upon employment status. Access revocation is immediately and automatically triggered by changes to status of employees or contractors in the HR system.
Vulnerability Management	**Vulnerability Scanning** Honeywell uses a standardized vulnerability management tool to scan, report, and check for compliance against common vulnerabilities, newly identified vulnerabilities and open services. Complete internal and external vulnerability scans are conducted monthly. **Penetration Testing** Honeywell's Center of Excellence (COE) for penetration testing (red and purple teams along with added technology assessments function) continually test and evaluate through research and application of innovative security technologies. **Remediation and Patch Management** Maintain remediation and mitigation plans for identified vulnerabilities and corresponding corrective measures. Asset owner documents acknowledgement of the risk and the IT business manager reviews and approves the remediation plan. Systems are maintained on a monthly patch cycle. System software components such as applications, database management systems, and web server software undergo security patches and version upgrades as means of software maintenance.
Incident Management	**Incident Response Plans** Maintain incident response plans. Incident response procedures exist for security and data protection incidents, which includes incident analysis, containment, response, remediation, reporting and the return to normal operations. **Incident Identification and Reporting** 24/7 Security Operations Center with array of tools and technologies for logging, detection, and analysis of system usage with rapid reporting requirements in accordance with US DoD DFARS 252.204-7012. **Supplier Incidents** Honeywell manages supplier incidents per reporting requirements in DFARS 252.204-7012.
Business Continuity Management	**Resilience** Replicate stored data between core data centers to add resiliency and further protect the data. Backups include data deemed necessary for full system restoration on business-critical systems. **Backup and Recovery** Routine back-up of databases and systems. Backup frequency is dictated by a standard rotation which is used globally within the Honeywell environment Backup and store data on local disk storage systems to allow for quick recovery in the event of a restore request. **Emergency Response and Disaster Recovery Plans** Maintain business continuity and disaster recovery plans to ensure a minimum level of continuity for the delivery of critical products and services during a significant interruption.
Supply Chain Risk Management	**Vetting** Complete due diligence and vetting procedures on third party vendors and contractors including review of relevant cyber and physical controls prior to granting access to Honeywell assets. **Non-Disclosure Agreements**

Categories	Practices
	Contractors and other third parties with access to networks are required to sign a non-disclosure agreement. **Security Requirements** Security terms and conditions are based on the scope of the product or service to be provided to Honeywell and the type of access required, including all applicable Honeywell security policies. **Supplier Risk Management** Risk assessments of Suppliers are conducted for any agreement where a Supplier will need access to a Honeywell asset, either physical (building, site, computer, etc.) or cyber (information asset) in order to fulfill the agreement.