Annex 2

Tridium Information Security Measures

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

Tridium has implemented the described measures across the Tridium 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 Tridium 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 Tridium 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

Categories	Practices
	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. **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.

Categories	Practices
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** Tridium 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** 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. Tridium 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. Tridium 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 Tridium email domain, and this helps prevent spam, spoofing and phishing.

Categories	Practices
	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 Tridium 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. **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

Categories	Practices
	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** Tridium'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. **GDRP 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. **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**

Categories	Practices
	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 Tridium-approved, encrypted removable media, by exception, which ensures a connection with the owner. **Data Termination** Upon written request, Tridium 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 Tridium retention policy. **Surveillance** Where necessary, security cameras and security guards are utilized to observe and enforce access controls, protection of Tridium employees, and Tridium property. **Intrusion Detection and Prevention** The audit trail of activities captured via CCTV or access control systems is retained for a

Categories	Practices
	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; • 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** Tridium 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** Tridium'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** Tridium manages supplier incidents per reporting requirements in DFARS 252.204-7012.

Categories	Practices
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 Tridium 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 Tridium assets. **Non-Disclosure Agreements** 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 Tridium and the type of access required, including all applicable Tridium security policies. **Supplier Risk Management** Risk assessments of Suppliers are conducted for any agreement where a Supplier will need access to a Tridium asset, either physical (building, site, computer, etc.) or cyber (information asset) in order to fulfill the agreement.

REVISION HISTORY:

Effective Date	Version	Description of Change	Section(s) Affected
27th October 2021	1.0	Document created	All
10th June 2022	2.0	Reordered topics/sections to be consistent with other documents, added statements to address customer questions.	All