SECURITY PRACTICES

These security practices (the "**Security Practices**") describe the technical and organizational security measures designed to protect and secure our SaaS Offerings under the Agreement and are incorporated into and form part of the Agreement. We may update the Security Practices from time to time provided that such updates do not result in a material degradation of the overall security of the Offering.

CATEGORIES	PRACTICES
Policy & Risk Management	• Tridium maintains an information security policy framework designed to safeguard the confidentiality, integrity, and availability of information assets. • Tridium maintains a documented risk management program that includes periodic risk assessment overseen by senior executive management and the security, legal, and audit functions.
Personnel Security	• Tridium personnel engaged in data processing are under a written obligation of confidentiality and are prohibited from collecting, Processing or using Personal Data without authorization. • Tridium's Global Data Privacy Policy requires employees to comply with Data Protection Laws with respect to the processing of Personal Data. • Tridium conducts or obtains background checks, where allowed by local law and reasonable for job roles, which may include educational, employment, and identity verification. • Tridium's compliance training includes a requirement for employees to complete an online course and pass an assessment covering information security and data privacy. • Tridium maintains an established set of procedures designed to ensure all staff promptly report actual and/or suspected security events. • Subprocessors with access to Tridium networks and systems are required to sign a non-disclosure agreement. • Due diligence and vetting procedures on third party vendors and contractors.
Data Handling	• Tridium uses commercially standard cryptography and security protocols to protect the confidentiality and integrity of customer data, including data-in-transit using TLS and full disk encryption for data-at-rest. • Cryptographic keys are managed according to defined policies, which include segregation of duties. • Multi-tenant applications hosted on cloud are segregated logically and data flow between various components of the platform is restricted within required subnets and VNETs. • Tridium maintains appropriate data security controls including: (i) identity and access management controls; (ii) periodic access reviews; (iii) role-based access (least privilege); (iv) secure log-in with unique user-ID/password; (v) complex password requirements; (vi) inactivity timeout requiring re-authentication; and (vii) auditing and logging of access to production data.
Operations Security	• Security monitoring solutions designed to detect and alert suspicious activities. • Change management process for IT systems and applications. • Tridium has a centralized patch management process to identify, evaluate, report and deploy patches and system updates.
Incident Management	• Incident response procedures exist for security and data protection incidents, which includes incident analysis, containment, response, remediation, reporting and the return to normal operations. • Tridium implements logging and analysis of system usage. • Chain-of-custody procedures while collecting evidence.
Backup	• Backups are performed on a periodic basis, encrypted, and stored off-site.
Business Continuity	• Tridium maintains a business continuity framework and disaster recovery plans to ensure a minimum level of continuity for the delivery of critical products and services during a significant interruption.
Network Security	• Network perimeter security through intrusion detection and prevention systems, routers and state of the art firewalls, and vulnerability scanning. • Anti-malware and anti-virus mechanisms.

CATEGORIES	PRACTICES
Third Parties	• Tridium uses industry-leading cloud providers for our cloud computing infrastructure. • Tridium leverages the controls of cloud providers. • Tridium uses commercially reasonable efforts to ensure that third-party suppliers and licensors to the Offering conform to substantially similar standards and levels of security as described in this Policy.
Certifications	• Certain SaaS offerings have third party security certifications (including SOC 2 and ISO) if stated in the Order Form.