SECURITY STANDARDS - MINIMUM INFORMATION TECHNOLOGY AND CYBER SECURITY REQUIREMENTS

Control	Requirements	Applicable Modules
Patch Management	Supplier and its Material Subcontractors must ensure that the latest available security updates and patches to all software used in the provision and/or support of the Services are promptly applied.	• Consulting & General Services Module • Goods (IT & non-IT) Purchase Module • Software Licence Module • SaaS Module • Telco Services Module • Co-lo Services Module • IT Reseller Module • Recruitment Services Module • Construction Services Module
Anti-Virus Software	Supplier and its Material Subcontractors must: (i) screen the Deliverables (immediately prior to their being made available to Morgan Stanley) using, and in the provision of the Services continuously use, a leading, commercially available software security program to detect the presence of any Virus and, upon detection, immediately eradicate or quarantine such Virus; and (ii) ensure that the Services do not contain any code or protocol that would: ▪ permit the gaining of unauthorized access to, or surreptitious monitoring of the use or operation of, the Deliverables or any System; or ▪ disable or impair the Deliverables or any System, in any way, based on the elapsing of a period of time, the exceeding of an authorized number of copies or scope of use or the advancement to a particular date or other numeral.	• Consulting & General Services Module • Goods (IT & non-IT) Purchase Module • Software Licence Module • SaaS Module • Telco Services Module • Co-lo Services Module • IT Reseller Module • Recruitment Services Module • Construction Services Module
Firewall	Supplier and its Material Subcontractors must ensure that a firewall is maintained in defense of all internet-facing systems used in the provision and/or support of the Services.	• Consulting & General Services Module • Goods (IT &

		non-IT) Purchase Module • Software Licence Module • SaaS Module • Telco Services Module • Co-lo Services Module • IT Reseller Module • Recruitment Services Module • Construction Services Module
Encryption Algorithms	Supplier and its Material Subcontractors must encrypt Morgan Stanley's Confidential Information in transit and at rest, using one or more of the following approved protocols and cryptographic algorithms: • Encryption in transit: TLS 1.2 or above, IPSec, SSHv2. • Encryption at rest: Symmetric Encryption using AES128, AES192, or AES256 in the CBC, CFB, OFB, CTR, XTS or GCM block cipher modes. Implementation notes: • If public key is used, it must be RSA-2048, RSA-3072, or RSA-4096. • If digital signature is used, it must be DSA-2048, DSA-3072, RSA-2048, RSA-3072, RSA-4096, ECDSA-224, ECDSA-256, ECDSA-384 or ECDSA-521. • If hashing algorithm is used, it must be SHA-256, SHA-384, SHA-512, SHA-512/256, SHA3-256, SHA3-384 or SHA3-512. • If key derivation function is used, it must be Argon2, PBKDF2, scrypt, or bcrypt.	• Consulting & General Services • Software Licence • Software-as-a-Service • Data & Subscription Services
Application-Level Encryption	Supplier and its Material Subcontractors must use application-level encryption to encrypt Morgan Stanley's Confidential Information at rest (rather than, e.g., self-encrypting drives, volume encryption or database encryption).	• Consulting & General Services • Software-as-a-Service • Data & Subscription Services
Key Management	Supplier and its Material Subcontractors must ensure that: • all encryption keys used in conjunction with Morgan Stanley's Confidential Information are dedicated to Morgan Stanley (and not used in conjunction with data of any other customer of Supplier); • all such encryption keys must be rotated at least once every two years; and • all such encryption keys must be stored in a designated vault or key management service, following industry best practices (e.g. NIST 800-57, FIPS140-2 level 2).	• Consulting & General Services • Software-as-a-Service • Data & Subscription Services

Authentication	Supplier and its Material Subcontractors must use multi-factor authentication for authenticating Morgan Stanley's Personnel or other authorized users attempting to access Morgan Stanley's Confidential Information or Systems.	• Consulting & General Services • Software-as-a-Service • Data & Subscription Services
Password updating	Supplier and its Material Subcontractors must ensure that Supplier Personnel accessing Morgan Stanley's account(s) with Supplier are regularly required to update their passwords.	• Consulting & General Services • Software-as-a-Service • Data & Subscription Services
Identity and Access Management	Supplier and its Material Subcontractors must ensure that the following identity and access management operations in respect of Morgan Stanley's Personnel or other authorized users accessing the Services can be controlled by Morgan Stanley (and not solely by Supplier): • User provisioning operations (e.g. create, modify, terminate, delete); • Entitlement management (e.g. create, modify, delete, assign and revoke roles and privileges); • Reporting for identity and access management operations (for the purpose of auditing and periodic reviews). These actions must take effect immediately on Morgan Stanley's request, either through administrator action or through automation.	• Consulting & General Services • Software-as-a-Service • Data & Subscription Services
Access Privileges	Supplier and its Material Subcontractors must ensure that access privileges are well defined and at a sufficient level of granularity to ensure that Morgan Stanley's users are only permitted the access they need. Supplier must ensure that administrator privilege access by Supplier Personnel to Morgan Stanley's account(s) with Supplier (i.e. ability of a user to modify asset configuration or controls (e.g. access management, logging etc.) beyond normal daily business use) is provided just in time, as needed, instead of persistently available.	• Consulting & General Services • Software-as-a-Service • Data & Subscription Services
User Activity Logs	Supplier and its Material Subcontractors must ensure that all activities by Supplier Personnel accessing Morgan Stanley's account(s) with Supplier are logged (such that the individual users who performed them are identifiable), that such logs are monitored, are secured to prevent unauthorized modification or deletion and retained for a period commensurate with the criticality of the operations concerned (without prejudice to Supplier's record retention obligations under the Agreement).	• Consulting & General Services • Software-as-a-Service • Data & Subscription Services
Penetration Testing	Supplier and its Material Subcontractors must ensure, for all Products and/or Services hosted by or on behalf of Supplier, that security penetration testing (or similar vulnerability threat testing) of the systems used in their provision to Morgan Stanley is performed, at least annually, and must provide Morgan Stanley with a summary of the results. Supplier must promptly remediate all vulnerabilities revealed by any of the foregoing testing. For Products and/or Services not hosted by or on behalf of	• Consulting & General Services Module • Goods (IT & non-IT) Purchase Module • Software Licence Module • SaaS Module

	Supplier, Supplier must permit Morgan Stanley (either itself or using a third party agreed between the parties) to perform (at Morgan Stanley's cost) security penetration testing (or similar vulnerability threat testing) of such Products and/or Services, to a scope to be pre-agreed between the parties. Supplier must promptly remediate all vulnerabilities revealed by any of the foregoing testing.	• Telco Services Module • Co-lo Services Module • IT Reseller Module • Recruitment Services Module • Construction Services Module
Quantum Security	Suppliers and its Material Subcontractors must identify and assess (at least annually) cryptographic algorithms and protocols used within the Services, and within any identity or access management products or services that Supplier or any of its Material Subcontractors utilises and implement and update (at least annually) quantum-resistant technologies in accordance with industry standards. • PQC Algorithms for Generation and Verification of Digital Signature Algorithms: o ML-DSA-44 o ML-DSA-65 o ML-DSA-87 o SLH-DSA-SHA2-128s o SLH-DSA-SHAKE-128s o SLH-DSA-SHA2-128f o SLH-DSA-SHAKE-128f o SLH-DSA-SHA2-192s o SLH-DSA-SHAKE-192s o SLH-DSA-SHA2-192f o SLH-DSA-SHAKE-192f o SLH-DSA-SHA2-256s o SLH-DSA-SHAKE-256s o SLH-DSA-SHA2-256f o SLH-DSA-SHAKE-256f • PQC Asymmetric Data Encryption and Data Decryption: o ML-KEM-512 o ML-KEM-768 o ML-KEM-1024	• Consulting & General Services Module • Goods (IT & non-IT) Purchase Module • Software Licence Module • SaaS Module • Telco Services Module • Co-lo Services Module • IT Reseller Module • Recruitment Services Module • Construction Services Module
Components Deployed On-Prem	Supplier and its Material Subcontractors must ensure that software supplied (or otherwise made available) by or on behalf of Supplier (or any of its Affiliates) that is deployed on any System does not require permanent privileged access on the host (e.g. root access on Linux, or local administrator access on Windows), but rather runs under a user specified non-privileged account.	• Consulting & General Services • Software Licence • Software-as-a-Service • Data & Subscription Services
	Supplier and its Material Subcontractors must ensure that software and firmware updates to, and new versions of, software supplied (or otherwise made available) by or on behalf of Supplier (or any of its Affiliates) that is deployed on any System do not auto-update or download automatically without following a change control process controlled by Morgan Stanley.	