**Annex A: General Security Requirements for Third Party vendors, partners and Service Providers.**

This annex outlines the minimum-security requirements expected of all third parties, including suppliers, service providers, and partners, engaged by MIC1. These requirements apply to any party with access to MIC1’s systems, data, or infrastructure, either directly or through subcontracted arrangements.

**1. Compliance and Governance**

* The Supplier shall comply with all applicable data protection and cybersecurity laws, regulations, and industry standards (e.g., ISO 27001, NIST CSF, local regulations) as well as GSMA security and privacy guidelines, where applicable and as relevant to the scope of services provided.
* The Supplier shall adhere to MIC1’s security policies, standards, and procedures, as communicated from time to time and any additional guidelines communicated during the term of the Agreement.

**2. Access Management**

* Access to MIC1 systems, platforms, or environments shall be granted on a need-to-know and least-privilege basis.
* All remote access must be protected using Multi-Factor Authentication (MFA) and established VPN solutions approved by MIC1.
* Supplier shall implement role-based access control (RBAC) and maintain a list of authorized personnel with periodic reviews.
* The use of shared or generic credentials is strictly prohibited. Credential lifecycle must be properly managed, including expiry, rotation, and revocation protocols.

**3. Third-Party and Subcontractor Security**

* The Supplier shall obtain prior written approval from MIC1 before engaging any subcontractor to perform any part of the contract.
* The Supplier shall ensure all subcontractors comply with the same security requirements as outlined herein.
* Supplier remains fully accountable for the actions and compliance of any subcontractor involved in delivering services under this Agreement.

**4. Data Protection and Information Handling**

* The Supplier shall ensure all personal, confidential, and proprietary information is protected in accordance with applicable laws and MIC1’s data handling policies.
* All sensitive data must be encrypted in transit (using TLS 1.2 or higher) and at rest (using AES-256 or equivalent).
* Data shall be stored, processed, and retained only within approved jurisdictions. Any cross-border data transfer must be subject to MIC1’s written approval and relevant legal safeguards.
* Upon contract termination or at the request of MIC1, the Supplier shall return or irreversibly destroy all data and provide a certificate of data destruction.

**5. Incident Detection and Response**

* The Supplier must promptly (within 24 hours) notify MIC1 of any actual or suspected security incident, including unauthorized access, data breach, malware infection, or credential compromise.
* A joint incident response process shall be established for coordinated handling of security events.
* Supplier shall maintain audit logs of all access and security-related events and share them with MIC1 upon request during incident investigation.

**6. Audit Rights and Security Assessments**

* MIC1 reserves the right to perform periodic security audits, assessments, or request independent third-party certifications related to the Supplier’s services.
* The Supplier must complete security due diligence questionnaires or risk assessments when requested by MIC1.
* Any identified security gaps must be remediated based on a mutually agreed timeline.

.**7. Training and Awareness**

* The Supplier shall ensure all personnel with access to MIC1 environments are adequately trained on cybersecurity, data protection, and acceptable use policies.
* Annual refresher training must be conducted, and records of completion shall be maintained and made available upon request.

**8. Termination, Exit Strategy, and Data Handling**

* Upon contract termination or expiration, Supplier shall:
	+ Revoke all access to MIC1 systems.
	+ Return or securely destroy all data and assets belonging to MIC1.
	+ Support transition activities as per the agreed exit plan.
* The Supplier shall certify data deletion within 30 days of contract termination.

**9. Liability and Enforcement**

* The Supplier shall be held liable for any damages, losses, or regulatory penalties resulting from breach of the above security obligations.
* Repeated or material non-compliance with security requirements may result in contract termination or penalties, as defined in the main Agreement.