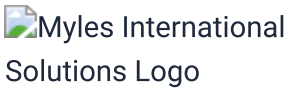
CORPORATE POLICY — MISL-POL-INFOSEC-05

Information Security, Confidentiality & OEM IP Protection Policy



Myles International Solutions Limited (RC 1687677) | Port Harcourt, Rivers State, Nigeria

Policy ID: MISL-POL-INFOSEC-05 | **Standards:** ISO 27001 Principles, Nigeria Data Protection Act (NDPA) | **Custodian:** ICT Manager

Information Protection Mandate: Myles International Solutions Limited (MISL) safeguards proprietary OEM engineering designs, distributor discount schedules, commercial tender pricing, and client reservoir/facility datasheets against unauthorized access, partner leakage, or cyber compromise.

1. OEM INTELLECTUAL PROPERTY & NON-CIRCUMVENTION CONTROLS

- **Restricted Access to OEM Proprietary Data:** Foreign OEM sizing software, P&IDs, cross-sectional valve/compressor drawings, and distributor discount structures are classified as *Strictly Confidential* and restricted solely to authorized MISL project personnel bound by Non-Disclosure Agreements (NDAs).
- **Partner Data Compartmentalization:** When transmitting technical datasheets to EPC consortium partner Ronngate Limited or subcontracted Port Harcourt workshops (PE Energy, Chilato-JUL, Vintex Technology), commercial OEM net pricing, agency commission schedules, and direct factory sales contacts must be redacted unless governed by an executed Non-Circumvention, Non-Disclosure Agreement (NCNDA).

2. DIGITAL HYGIENE, ACCESS CONTROL & DATA BACKUP

- **Official Corporate Domains & MFA:** All official business correspondence with oil majors, foreign OEMs, and government regulators must be conducted exclusively through corporate `@myleslimited.com` email accounts protected by mandatory Multi-Factor Authentication (MFA) and complex password rotation. Personal email accounts shall never be used for tender or OEM business.
- **Encrypted Cloud Repository & Backups:** All active tender packages, signed OEM Letters of Authorization (LOAs), NUPRC permits, and QA/QC certification dossiers must be stored on encrypted, role-restricted corporate cloud drives with automated daily off-site backups managed by the ICT Manager.
- **Endpoint & Portal Credential Security:** Corporate laptops and mobile devices accessing NIPEX, NOGICJQS, or IOC e-procurement portals must enforce full-disk encryption, automatic screen lock, and immediate credential revocation upon staff separation.

3. DATA CLASSIFICATION & HANDLING MATRIX

Classification Tier	Document & Data Examples	Mandatory Security & Sharing Control
Tier 1: Strictly Confidential	OEM net factory quotes, agency agreements, consortium revenue splits, NIPEX/portal passwords.	Restricted to MD and cleared executives; encrypted storage; never shared externally without NCNDA.
Tier 2: Commercial / Technical	Client RFQs, P&IDs, sizing datasheets, Port Harcourt workshop ITPs and calibration scopes.	Role-based cloud access; commercial margins redacted prior to subcontractor transmission.
Tier 3: Corporate & Public	Published Corporate Profile, NUPRC permit summaries, website brochures, HSE policy statements.	Approved for external distribution to prospective clients, OEMs, and tender pre-qualification portals.

4. EXECUTIVE PROMULGATION & APPROVAL

Approved & Promulgated By:	**Information Security & IT Custody:**
Andrew Okechukwu Okwedadi Managing Director / Chief Executive Officer Myles International Solutions Limited	**Frank Okwedadi** ICT & Digital Systems Manager Document Control Ref: MISL-POL-INFOSEC-05-REV2