PARAMOUNT COMMUNICATIONS LIMITED
(CIN: L74899DL1994PLC061295)

IT Security, Infrastructure
&
Governance Policy
of
Paramount Communications Limited

****

1. Purpose

This policy establishes a unified framework to safeguard the company's IT infrastructure, data, and digital assets.
It aims to:

- Protect information systems from cyber threats and misuse
- Ensure business continuity, regulatory compliance, and cyber resilience
- Minimize cyber, operational, and compliance risks
- Support secure digital transformation and AI-led initiatives

---

2. Scope

This policy applies to:

- All servers, endpoints, networks, and data centres
- User identities, access rights, and mobile devices
- Microsoft 365, cloud platforms, and Mobile Device Management (MDM)
- Business applications (excluding ERP systems)
- Employees, contractors, and third-party service providers

---

3. Key Control Pillars

3.1 Infrastructure & Server Security

- Periodic security, vulnerability, and configuration assessments
- Operating system hardening, timely patching, backups, and continuous monitoring
- High Availability (HA) and Disaster Recovery (DR) for business-critical systems

3.2 Identity & Access Management (IAM)

- Role-based, least-privilege, and need-to-know access controls
- Mandatory Multi-Factor Authentication (MFA) for privileged and remote access
- Immediate revocation of access upon employee exit or role change

3.3 Endpoint & Device Security

- Standardized antivirus/EDR, encryption, and host firewall across all endpoints
- Controlled and monitored use of external storage devices
- Network access restrictions for non-compliant or unmanaged devices

3.4 Microsoft 365 & Mobile Security

- Enforcement of MFA, Conditional Access, Data Loss Prevention (DLP), and audit logging
- Mandatory MDM enrollment for all corporate and BYOD mobile devices
- Remote lock and wipe capabilities for lost, stolen, or compromised devices

3.5 Network & Data Center Security

- Controlled physical access with monitoring and redundancy
- Secure baseline configurations for firewalls, switches, and wireless networks
- Periodic review and cleanup of firewall rules and Wi-Fi access policies

3.6 Application Security (Non-ERP)

- Secure development, testing, and deployment standards
- Mandatory security testing before production release
- Encryption, logging, and protection of sensitive business data

3.7 Governance, Risk & Compliance

- Alignment with applicable legal, regulatory, and internal compliance requirements
- Periodic audits, risk assessments, and corrective action tracking
- Defined incident reporting, response, and remediation process

---

4. Roles & Accountability

- **Board & Senior Management:** Strategic oversight and governance
- **IT & Information Security:** Policy implementation, monitoring, and enforcement
- **Employees & Users:** Compliance with security policies and practices
- **Vendors & Partners:** Adherence to company security and compliance standards

---

5. Business Value

- Reduced cyber, operational, and compliance risks
- Improved audit readiness and regulatory confidence
- Protection against data breaches, system downtime, and financial loss
- Strong and secure foundation for digital growth and AI adoption

---

6. Review & Enforcement

- This policy shall be reviewed annually or upon significant technology, business, or regulatory changes
- Non-compliance may result in access suspension, disciplinary action, or contractual penalties

---