Information Security Program Management

Public

At UPL, we recognize that information security and cyber resilience are fundamental to protecting stakeholder trust, ensuring operational continuity, and supporting sustainable business growth across all regions.

We have established and maintain a comprehensive Information Security Management Program (ISMP) aligned with globally accepted standards and industry best practices to safeguard our information technology infrastructure, data assets, and digital operations.

1. **Governance & Standards**

   Our Information Security Management Program is aligned to:

   - ISO/IEC 27001:2022 Information Security Management System
   - NIST Cyber Security Framework (CSF)
   - Industry best practices for cyber resilience, risk management, and data protection
   - Internal governance frameworks monitored by the CISO function

2. **Scope of the Information Security Management Program**

   The program covers, but not limited to, the following key elements across UPL entities and operations:

   - Information Security related Business Continuity Plans: Information security–driven business continuity plans to ensure resilience of critical systems and data.
   - Vulnerability Management: Continuous vulnerability assessment, penetration testing, and remediation processes.
   - Internal Audits: Periodic internal audits of IT infrastructure and ISMS controls.
   - Independent External Audits: External ISO 27001 audits and assessments of security controls.
   - Incident Reporting & Escalation: Defined escalation mechanism for employees to report incidents, vulnerabilities, or suspicious activities to Cyber Security function.
   - Security Awareness: Mandatory information security awareness training for all employees annually.

- Risk Management: Information security risk assessments integrated into enterprise risk management.
- Technology Infrastructure Security: Protection of information assets such as hardware, software, networks, and stored data from threats and disruptions.
- Transparency on Security Incidents: UPL maintains transparency and governance discipline in reporting material information security incidents. Total number of material information security breaches in the last financial year: None

UPL remains committed to continuously strengthening its cyber resilience posture to protect stakeholder data, ensure operational continuity, and support sustainable growth.

UPL LIMITED MUMBAI

Manoj Kumar Shrivastava

(Chief Information Security Officer)

Pushkar Rege

(Global Chief Information Officer)