Dataco Global Technology Adoption Policy

Purpose

This policy establishes clear standards for the adoption and management of emerging technologies (including Internet of Things (IoT), Blockchain, and related innovations) within Dataco Global. It ensures all technology use aligns with company objectives, emphasizes security, safeguards data, and supports operational excellence through measurable controls and responsibilities.

Scope

This policy applies to all employees, contractors, partners, and third-party service providers involved in the selection, deployment, management, and operation of IoT, Blockchain, and similar technologies within Dataco Global's business processes.

1. Technology Evaluation and Approval

- All new technology projects must undergo a standardized evaluation, including risk assessment and Return on Investment (ROI) analysis, before approval.
- A minimum of two formal pilot tests, each covering at least 10% of the relevant operational environment, are required prior to full-scale deployment.
- The Technology Steering Committee (TSC) must approve any expenditure over $100,000 or any project impacting more than 25% of company data infrastructure.

2. Data Governance and Protection

- Data collected or generated by IoT devices and Blockchain applications must be classified according to Dataco Global's data governance standards (confidential, internal, public).
- Only authorized personnel (not exceeding 20% of departmental staff per project) may access sensitive or confidential data[4].
- Encryption must be applied to all data transmissions involving IoT devices and Blockchain transactions.
- All data must be retained only as long as necessary for business or regulatory requirements, with quarterly reviews to ensure compliance[5].
- At least one Data Steward must be assigned to each project to oversee data ownership, access controls, and compliance[4].

3. Security and Compliance

- All devices and systems must undergo penetration testing at least twice annually.
- Any technology solution must comply with applicable industry standards (e.g., ISO 27001) and regulatory frameworks (e.g., GDPR, CCPA).

- Incident response protocols must be in place, with a maximum incident response time of 4 hours for critical breaches.
- Multi-factor authentication is mandatory for administrative access to IoT, Blockchain, and associated management platforms.

4. Performance and Reliability

- IoT systems must achieve at least 99.5% uptime; Blockchain nodes must have a minimum of two redundant nodes per key business network.
- All deployed technologies must be reviewed bi-annually for performance, with a target of less than 1% device or node failure rate.

5. Vendor and Third-Party Management

- All vendors providing IoT or Blockchain services must sign a data protection agreement and undergo an annual security audit.
- No more than 30% of critical infrastructure may depend on a single third-party provider to mitigate operational risks.

6. Training and Awareness

- All users must complete an approved training module on responsible technology use and security before gaining access to relevant platforms. A refresher course is required every 12 months.
- At least 95% of identified stakeholders must complete their training within 60 days of technology rollout.

7. Monitoring and Reporting

- Continuous monitoring solutions must be deployed for all IoT and Blockchain systems to detect anomalies or unauthorized access, with alerting thresholds set according to impact risk.
- Quarterly reports on usage, incidents, and compliance must be submitted to senior management.

> **Note:** This policy has been generated specially for the hackathon. It has no relation with Syngenta or any other company.