Dataco Global Data Security and Cybersecurity Policy

Purpose
This policy defines the mandatory rules and procedures for ensuring the confidentiality, integrity, and availability of Dataco Global's data, technology infrastructure, and related information assets. The goal is to minimize risks from human error, system malfunction, and malicious cyber activity by implementing best-practice controls and quantifiable standards[2][5].

Scope
This policy applies to all employees, contractors, third-party vendors, interns, and visitors with temporary or permanent access to Dataco Global’s systems, networks, or physical premises[5].

1. Access Management and Controls

- All user accounts must employ Multi-Factor Authentication (MFA) and strong password protection: passwords must be at least 12 characters, include upper and lower case letters, numbers, and symbols[1].
- User access must follow the principle of least privilege. Employees are granted access only to the information necessary for their job role. Quarterly reviews will audit access levels for 100% of users to ensure compliance[1].
- User session timeouts must be enforced after 15 minutes of inactivity, with automatic log-off to prevent unauthorized access[1].
- All failed login attempts above five within a 24-hour period will result in account lockout for a minimum of 30 minutes and trigger an automated security alert.

2. Data Classification and Protection

- All company data must be classified into: Public, Internal, Confidential, and Restricted.
- Confidential or Restricted data must be encrypted both in transit (using a minimum of TLS 1.3) and at rest (using AES-256 encryption as standard)[2].
- No more than 5% of company data can be stored unencrypted at any given time; regular scans will verify compliance every month.
- Physical access to servers and data centers is restricted to authorized personnel only and requires badge access, with logs retained for at least 12 months.

3. Network Security

- Firewalls must be deployed at all external network boundaries, with port scanning and intrusion detection systems (IDS) monitoring traffic 24/7[2].

- All software and firmware must be updated and patched within 7 business days of release for critical vulnerabilities.
- Remote access to company systems must use VPN with 256-bit encryption, and connections from untrusted networks are automatically blocked.

4. Incident Response

- All employees must report suspected security incidents within 15 minutes of discovery to the IT Security Team via a dedicated channel[1].
- Incident response procedures must be tested twice a year through tabletop or live simulation exercises.
- The IT Security Team must begin containment and assessment of high-severity incidents within 1 hour of detection, and external breaches must be disclosed to leadership within 24 hours[1].

5. Training and Awareness

- All employees and contractors must complete cybersecurity awareness training within 30 days of hire and participate in annual refresher courses; compliance rate must exceed 98% company-wide.
- A minimum of 5 simulated phishing exercises will be conducted per year; any employee failing more than two will receive additional training.

6. Data Retention and Disposal

- Company data classified as Confidential or Restricted must be retained for no longer than 7 years unless legally required.
- Secure data destruction methods (e.g., shredding, wiping with DoD 5220.22-M standard) are required for all data and devices being decommissioned, with 100% compliance documented.

7. Audit and Compliance

- Quarterly internal audits will verify adherence to this policy, with results reported to executive management. Any critical non-compliances must be remediated within 14 business days.
- External audits for compliance with applicable regulations (e.g., GDPR, HIPAA) will be conducted at least annually.

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