

# Dataco Global: Risk Management and Mitigation Policy

---

## 1. Purpose

This policy establishes a structured approach for identifying, assessing, managing, and mitigating risks at Dataco Global. The aim is to protect company assets, ensure business continuity, and support the achievement of strategic objectives[2][5].

## 2. Scope

This policy applies to all Dataco Global employees, contractors, suppliers, and business partners across all departments and locations[2][5].

## 3. Objectives

- Identify, assess, and manage risks that could affect Dataco Global's operations, reputation, and compliance.
- Establish clear risk tolerances and appetites to guide decision-making.
- Ensure regular reporting and review of risks and controls[3][5].
- Promote a risk-aware culture throughout the organization.

## 4. Risk Appetite and Tolerances

- Dataco Global will not tolerate financial losses exceeding 3% of annual company revenue in any given fiscal year.
- Cybersecurity incidents leading to data breaches must not impact more than 100,000 unique customer records per event.
- Acceptable downtime for critical systems is limited to 4 hours per incident, with no more than two incidents per quarter.
- The company will maintain a minimum business continuity reserve equivalent to 6 months of operational expenses[3].

## 5. Risk Management Process

- All business units must conduct risk assessments at least semi-annually.
- All identified risks must be analyzed, assigned an owner, and entered into the centralized risk register.
- Risks rated as "High" (scoring 16 or more on a 25-point scale) must have a mitigation plan created within 14 business days of identification[5].
- Mitigation plans must include quantifiable targets and deadlines, with updates tracked quarterly.

## 6. Integration with Business Processes

- Risk management will be embedded in business planning, performance management, project management, and business continuity strategies.
- Department heads must integrate risk considerations into all major business initiatives and routinely discuss them at monthly leadership meetings[5].

## 7. Risk Categories

Risks will be monitored and reported in the following categories:

- Strategic
- Financial
- Operational
- Technology/Cybersecurity
- Legal/Compliance
- Reputational
- Environmental/Health & Safety[5]

## 8. Risk Register

- All risks must be documented in the risk register, including risk description, category, owner, rating, mitigation actions, and review dates.
- The risk register will be reviewed and updated quarterly by the Risk Management Committee[5].

## 9. Reporting and Review

- The Chief Risk Officer will prepare consolidated risk reports for executive management and the Board on a quarterly basis[5].
- Risk appetite and tolerance levels will be reviewed and, if necessary, updated annually or when significant changes to the company's business model occur[3][5].
- Any breach of risk appetite or tolerance must be escalated to the Management Committee within 48 hours and reported to the Board at the next scheduled meeting[3].

## 10. Training and Awareness

All staff must complete mandatory risk management training within 30 days of joining Dataco Global and an annual refresher course thereafter.

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