Policy – Safeguarding Sensitive Information

Policy on Safeguarding Sensitive Information: Material Volumes, Procurement Details and Supply Chain Data

1. Purpose

This policy establishes the guidelines for safeguarding sensitive information related to material volumes, procurement details, and supply chain data to prevent competitive intelligence leaks or misuse. The policy applies to all employees, contractors, and third-party partners with access to such information.

2. Scope This policy covers:

- Material volume data
- Procurement details, including supplier agreements and pricing
- Supply chain logistics and related data
- Any other proprietary or confidential information related to the organisation's material inputs and operations

3. Definitions

- **Sensitive Information**: Any data or documentation classified as confidential, proprietary, or critical to the organisation's operations, including but not limited to material inputs, supplier agreements, pricing strategies, and logistics details.
- **Access Control**: Measures designed to regulate who can view or use sensitive information within the organisation.

4. Risks:

4.1. Data scraping (external)

Data scraping is a complementary tool in A.I. workflows. It automatically extracts information from online sources using software tools to gather large datasets, typically in a structured format for analysis and compilation into reports covering domains such as market size estimations, growth forecasts, competitor benchmarking, and sentiment analysis of customer feedback. Commercial research agencies monetise these reports through subscriptions or one-time purchases and are used by clients for strategic decision-making, investment analysis, competitive intelligence, or market entry planning. The practice often disregards legal frameworks, such as copyright protections, leading to potential violations.

Given the vast amount of published content, including articles and reports by Composites Australia Inc., the organisation is vulnerable to data scraping activities. There are risks of plagiarism, unreliable or misleading insights, and privacy concerns for personal information garnered by data scraping by commercial research agencies as well as Universities.

5. Policy Statements

5.1. Access and Control

- Access to sensitive information gathered by Composites Australia will be granted only to authorised personnel on a need-to-know basis.
- A formal process will be implemented to approve, review, and revoke access rights.

5.2. Data Storage and Protection

- Sensitive information must be stored in secure locations, whether physical (e.g., locked cabinets) or digital (e.g., encrypted systems).
- Digital data should be protected using secure systems with up-to-date encryption standards and access logs.
- Hard copies of sensitive information must be securely stored and shredded when no longer needed.

5.3. Communication and Sharing

- Sensitive information must not be shared via unsecured channels (e.g., personal email, unencrypted messaging platforms).
- Internal sharing must comply with access control guidelines, ensuring only authorised personnel receive the information.
- External sharing must be pre-approved by the relevant manager and covered by a legally binding non-disclosure agreement (NDA).

5.4. Monitoring and Compliance

- The organisation will regularly monitor access logs and data use to identify potential breaches.
- Any suspicious activity will be investigated promptly, and corrective actions will be implemented as necessary.

5.5. Incident Management

- Any breach of sensitive information must be reported immediately to the designated Data Protection Officer (DPO).
- An investigation will be conducted to determine the cause and impact of the breach.
- Measures will be taken to mitigate damage, and affected parties will be informed as required.

6. Roles and Responsibilities

- **Employees and contractors**: Ensure compliance with this policy and report any potential or actual breaches.
- **Board members:** Oversee the implementation and enforcement of this policy, conduct regular audits, and manage incident responses. Authorise access, monitor adherence to the policy, and escalate incidents as necessary.

7. Non-Compliance

Failure to comply with this policy may result in disciplinary actions, including termination of employment, and could lead to legal consequences depending on the severity of the breach.

8. Review and Updates

This policy will be reviewed annually or as necessary to ensure it remains effective and aligned with organisational needs and legal requirements.

9. Approval

This policy has been reviewed and approved by senior management and is effective as of [Date].

1. Responsibilities and Authorities:

- The Executive Director of C.A. is responsible for protecting sensitive data.

2. Linked Policies

- Branding Guidelines
- Social Media
- Use of A.I.
- Magazine Editorial and Content Policy

END