ZJLD Group
Information Security Policy

Version: A/0

Prepared by: Information Technology Center

Reviewed by: CEO

Approved by: Board of Directors

Released and effective on 1st Jan, 2022 by ZJLD Group Inc.

Chapter 1: General Provisions

Article 1
This Policy is established to strengthen information security at ZJLD and its subsidiaries (the "**Group**"), ensuring effective business operations and data privacy.

Article 2
This Policy applies to all employees of the Group.

Chapter 2: Information Security Management

Article 3: Roles and Responsibilities
3.1 The Group's Board (the "**Board**") of Directors (the "**Directors**") supervises overall information security.
3.2 Information Director appointed by the Board is responsible for overseeing information security strategy and governance, reporting major incidents to the Board.
3.3 The Information Director formulates the specific information security strategy and implements work plans.

Article 4: Information Data Classification and Management
4.1 Information is classified by materiality and sensitivity as follows:

- **L1:** Publicly available information (e.g., corporate website news, promotional articles).
- **L2:** Internally available information (e.g., internal newspaper contents, official documents).
- **L3:** Non-operational data, public third-party data, and desensitized personal information (e.g., customer visit records, channel customer data).
- **L4:** Operational data, non-public third-party data, detailed personal information, and employee management data (e.g., financial statements, production formulas).

4.2 Access to L1 and L2 data requires department head approval, while data asset managers oversee L3 and L4 data to prevent leakage, loss, or misuse. L3 and L4 data must be desensitized and encrypted upon approval.

Article 5: Information Security Training
5.1 Information security training is mandatory for all new hires.
5.2 Existing employees must receive training at least once a year.

Article 6: Information Assessment and Reporting
6.1 Employees must handle data assets responsibly. Disclosure, transfer, or misuse is prohibited. Information security incidents, such as data loss or leakage, will impact annual performance assessments. Responsible individuals may face disciplinary actions such as criticism and education, economic penalties or administrative actions depending on the severity of the circumstances. Those who violate relevant national laws or impose a significant impact on the Group will be referred to judicial authorities. Department heads will also be held accountable.

6.2 Employees must report any potential security risks or data incidents to the Information Centre (xxzx@zjld.com) promptly for investigation.

Chapter 3: Supplementary Provisions

Article 7
The Information Centre is responsible for interpreting this Policy.

Article 8
This Policy is approved by the Board and takes effect upon release.