VJDS International Inc. Confidentiality Policy

Effective Date: 20th March 2013
Approved By: Directors
Updated: 17th November 2024

1. **Purpose**
The purpose of this Confidentiality Policy is to protect sensitive and proprietary information, ensure the privacy and security of customer and employee data, and provide guidelines for employees, contractors, and third-party partners regarding their responsibilities to maintain confidentiality. This policy applies to all individuals who have access to confidential information, whether directly or indirectly, as part of their work at VJDS International Inc. This Policy is designed to safeguard sensitive and proprietary information within an organization. It sets out the expectations and obligations for employees, contractors, and third-party partners regarding the protection of confidential information, both during and after their employment or engagement with the company. This policy helps ensure that the company's trade secrets, business strategies, financial data, customer information, and other proprietary data are not improperly disclosed, used, or accessed.
The implementation of this policy is accompanied by regular employee training, secure systems for data management, and strict enforcement to prevent unauthorized disclosure or misuse of confidential information.

2. **Scope**
This policy applies to:
- All employees (full-time, part-time, temporary, and contract employees).
- Independent contractors, consultants, and service providers who may come into contact with confidential information.
- Any third parties, business partners, or affiliates who have access to confidential company data.

Confidential information includes, but is not limited to, the following categories:
- Business Plans and Strategies: Future plans, projections, marketing strategies, and business models.
- Financial Data: Financial statements, budgets, forecasts, and records of revenue or expenses.
- Employee Information: Personal data, compensation details, performance reviews, and other personnel-related information.
- Customer and Client Information: Customer contact details, contracts, orders, pricing, and payment history.
- Intellectual Property: Patents, trademarks, copyrights, trade secrets, product designs, and proprietary technologies.
- Software and Systems: Source code, algorithms, system architectures, databases, and software tools.
- Operational Information: Manufacturing processes, supply chain data, and any confidential business operations data.

3. **Confidentiality Obligations**
Employees, contractors, and third parties must:
- Maintain Confidentiality: Keep all confidential information secure and not disclose it to unauthorized individuals or entities both within and outside.

- Use Information Only for Intended Purposes: Use confidential information only for the purpose it was provided and in the course of fulfilling their job duties. Confidential information should not be used for personal benefit or to the benefit of third parties.
- Share Only on a Need-to-Know Basis: Disclose confidential information only to those within the organization who have a legitimate need to know and are authorized to receive the information.
- Take Necessary Precautions: Ensure that confidential information is physically and electronically secured. This includes using strong passwords, locking physical documents, and ensuring that information is not left unattended or easily accessible to unauthorized parties.
- Report Breaches: Immediately report any known or suspected breaches of confidentiality to management or the Data Protection Officer (DPO) to enable prompt action.

4. **Exceptions to Confidentiality**
There are certain circumstances where employees, contractors, and third parties may disclose confidential information:
- Legal Obligations: If required by law or regulation, confidential information may be disclosed to appropriate authorities or as part of a legal process, such as a court order or subpoena.
- Protecting Company Interests: If the disclosure is necessary to protect the company's interests (e.g., in the case of a business dispute or litigation), authorized individuals may share relevant information.

5. **Data Security Measures**
To protect confidential information, VJDS International Inc. has implemented the following data security measures:
- Physical Security: All physical confidential documents should be stored in locked files or secure cabinets. Employees are expected to ensure that documents containing confidential information are not left unattended in public areas.
- Electronic Security: Use of encrypted communication, strong passwords, and multi-factor authentication to protect access to company systems. Access to confidential data is granted based on the principle of "least privilege" (only the minimum level of access necessary for job performance).
- Remote Access: Employees working remotely or off-site must use company-provided VPNs and secure devices to access company networks and data.
- Training: Regular training on data protection, confidentiality, and security protocols to ensure employees understand how to handle sensitive information safely.

6. **Confidentiality After Employment**
Employees, contractors, and third-party partners have an ongoing obligation to protect the confidentiality of company information, even after their employment or contract ends. This includes:
- Non-Disclosure: Former employees, contractors, and business partners are prohibited from disclosing or using any confidential information they acquired during their employment or engagement.
- Return of Materials: Upon the termination of employment or contract, all physical and digital materials containing confidential information must be returned to the Data Protection Officer (DPO) of VJDS International Inc., and any unauthorized copies must be destroyed.
- Post-Employment Restrictions: Employees may be subject to non-compete, non-solicitation, or other post-employment restrictions that help safeguard confidential business information.

7. **Consequences of Violating the Confidentiality Policy**
Violating the confidentiality obligations outlined in this policy can result in serious consequences, including:

- Disciplinary Action: Employees who breach confidentiality may face disciplinary actions, up to and including termination of employment.
- Legal Consequences: Unauthorized disclosure of confidential information can result in legal action, including civil lawsuits or criminal penalties.
- Financial Liability: In some cases, employees or contractors may be held financially liable for damages resulting from the disclosure of confidential information.

8. **Non-Disclosure Agreements (NDAs)**
In certain cases, VJDS International Inc. may require employees, contractors, or third-party vendors to sign Non-Disclosure Agreements (NDAs) to formalize confidentiality expectations and clarify the scope of confidential information. The NDA will detail:
- The types of information deemed confidential.
- The obligations of the parties involved.
- The consequences of unauthorized disclosure.

9. **Confidentiality During and After Termination**
Upon termination of employment or the end of a contract, individuals must:
- Return all documents, files, or any other materials containing confidential information.
- Ensure that no confidential information is retained in personal devices, emails, or storage.
- Comply with any post-employment non-disclosure or non-compete agreements that are applicable.

10. **Policy Review and Amendments**
This Confidentiality Policy will be reviewed and updated as necessary to ensure compliance with legal requirements and industry best practices. Employees will be notified of any changes to the policy.