Information Security Policy

D.M. Wenceslao & Associates Inc. (DMW) is committed to protecting its information assets and the privacy of personal data. This Information Security Policy outlines our commitments to continuously improve security measures, ensure the integrity and protection of data, monitor and respond to security threats, assign clear security responsibilities across our workforce, and enforce security requirements with third-party partners. These commitments are aligned with our established Privacy Policy and IT Business Continuity Plan, reflecting our dedication to safeguarding information against unauthorized use, loss, alteration, or access and to complying with applicable data protection laws.

I. Continuous Improvement of Security System

We continuously improve our information security systems and processes. DMW adopts industry best practices and regularly evaluates its security controls to adapt to emerging threats and technologies. Additionally, our security policies and procedures are periodically reviewed and updated as needed to drive ongoing improvement in line with global standards and evolving risks.

II. Data Integrity and Protection

We ensure the integrity and protection of data through robust technical and organizational measures. All sensitive information is safeguarded against unauthorized access, alteration, destruction, or loss. In alignment with global data protection standards, our Data Privacy Policy is strictly followed to comply with relevant laws and to protect confidential information acquired through our business activities. Measures such as access controls, encryption, end point protection, email threat protection and adherence to principles like data minimization and purpose limitation are employed to preserve data confidentiality and accuracy. We also maintain data availability by performing regular backups, redundancies and disaster recovery planning, full backups are done daily (with additional incremental backups throughout the day) and backup copies are retained securely. These practices ensure that critical data can be restored and remain trustworthy even in the event of unforeseen incidents.

III. Monitoring and Responding to Security Threats

We monitor and respond to information security threats proactively. DMWAI's IT team continuously monitors networks and systems for signs of potential breaches, vulnerabilities, or unusual activities. Ongoing monitoring mechanisms enable us to promptly identify and address potential issues before they escalate. We have established incident response procedures to contain and resolve security incidents swiftly, minimizing damage and recovery time. In addition, we maintain comprehensive Business Continuity Plans and risk mitigation strategies to sustain operations during disruptions. These plans include redundant systems, regular offsite data backups, and tested recovery processes so that if a cyber-attack, system failure, or disaster occurs, we can quickly restore critical services and protect our data.

IV. Workforce Information Security Responsibilities

We assign individual responsibilities for information security to our entire workforce. Every DMW employee, contractor, and agent has a duty to uphold our information security policies and to protect the data they handle. We promote a strong security-aware culture through continuous training, clear communication, and reinforcement of policies, which fosters integrity and accountability in daily operations. All personnel are required to follow the company's security procedures and guidelines; access to sensitive data is strictly limited to those with a legitimate business need-to-know, and they may only process such data on our instructions under binding confidentiality agreements. We also encourage all staff to remain vigilant and immediately report any suspected security incidents or weaknesses. By making information security a shared responsibility, DMW ensures that every member of the organization contributes to the protection of our information assets.

V. Information Security Requirements for Third Parties

We extend our security requirements to all third-party service providers, suppliers, and business partners who handle our information. DMWAI carefully selects and manages vendors to ensure they meet our high security and privacy standards. Any third party with access to our systems or data must agree to comply with applicable laws (including the Data Privacy Act) and adhere to our internal security and privacy policies. We require such partners to maintain strict confidentiality of our information and to use the data only for authorized purposes. These expectations are formalized in our contracts and the Supplier Code of Conduct, and we perform regular supplier assessments or audits of critical third parties to verify ongoing compliance. By enforcing information security requirements with external parties, we ensure that our data remains protected throughout our supply chain and partner network.