

VERSION NO. 1	MANUAL TITLE SUSTAINABILITY POLICIES	DOCUMENT NO. SUST-POL-002
	DOCUMENT NAME INFORMATION SECURITY POLICY	REVISION NO. 0
		EFFECTIVITY DATE SEPTEMBER 09, 2026
		PAGE NO. 1 OF 4

1.0 INTRODUCTION

D.M. Wenceslao & Associates, Inc. (DMW) recognizes the importance of protecting its information assets and maintaining the confidentiality, integrity, and availability of information. The Company is committed to safeguarding information from unauthorized access, disclosure, alteration, loss, destruction, misuse, and other security threats.

This policy establishes the principles governing DMW's information security practices and supports the Company's commitment to responsible information management, business continuity, data privacy, cybersecurity resilience, and continuous improvement.

2.0 INFORMATION SECURITY COMMITMENTS

2.1 Information Security Governance

- 2.1.1 DMW maintains information security governance practices to support the protection of information assets and information systems.
- 2.1.2 Information security risks shall be considered as part of the Company's broader risk management and business continuity processes.
- 2.1.3 Information security incidents, vulnerabilities, and emerging threats shall be reported and addressed through appropriate management channels.
- 2.1.4 Information security governance is supported through oversight by the Audit and Risk Committee and management-level accountability through the Executive Committee, with relevant functions responsible for implementing information security controls and practices.

2.2 Continuous Improvement

- 2.2.1 DMW seeks to continuously improve its information security controls, processes, and practices to address evolving threats, technologies, and business requirements.
- 2.2.2 Information security policies, procedures, and controls shall be periodically reviewed and updated where appropriate.
- 2.2.3 Opportunities to strengthen information security resilience and risk management shall be evaluated on an ongoing basis.

2.3 Data Protection and Integrity

MASTER COPY

VERSION NO. 1	MANUAL TITLE SUSTAINABILITY POLICIES	DOCUMENT NO. SUST-POL-002
	DOCUMENT NAME INFORMATION SECURITY POLICY	REVISION NO. 0
		EFFECTIVITY DATE SEPTEMBER 09, 2026
		PAGE NO. 2 OF 4

- 2.3.1 DMW shall implement appropriate technical and organizational measures to protect information assets and maintain data confidentiality, integrity, and availability.
- 2.3.2 Access to sensitive information shall be restricted based on business need and authorized access rights.
- 2.3.3 Information shall be protected against unauthorized access, alteration, loss, destruction, disclosure, or misuse.
- 2.3.4 Information handling practices shall be aligned with applicable laws, regulations, and company policies relating to data privacy and information security.
- 2.4 Monitoring and Incident Response
 - 2.4.1 DMW seeks to proactively identify, monitor, and manage information security risks, vulnerabilities, and threats.
 - 2.4.2 Information security incidents shall be addressed through established response and recovery procedures designed to minimize operational disruption and potential impacts.
 - 2.4.3 Employees are expected to promptly report suspected information security incidents, vulnerabilities, or suspicious activities through established reporting channels.
 - 2.4.4 Lessons learned from information security incidents may be used to strengthen controls and improve security practices.
- 2.5 Business Continuity and Recovery
 - 2.5.1 DMW maintains business continuity and recovery arrangements to support the resilience and availability of critical information systems and services.
 - 2.5.2 Backup, recovery, and continuity measures shall be implemented to support operational resilience and reduce the impact of disruptions.
 - 2.5.3 Information security considerations shall be incorporated into business continuity planning and recovery activities.

3.0 INFORMATION SECURITY PROGRAMS

- 3.1 Information Security Awareness and Training
 - 3.1.1 DMW promotes a culture of information security awareness across the organization.

MASTER COPY

VERSION NO. 1	MANUAL TITLE SUSTAINABILITY POLICIES	DOCUMENT NO. SUST-POL-002
	DOCUMENT NAME INFORMATION SECURITY POLICY	REVISION NO. 0
		EFFECTIVITY DATE SEPTEMBER 09, 2026
		PAGE NO. 3 OF 4

3.1.2 Employees receive guidance, communications, awareness activities, or training on information security responsibilities, cybersecurity risks, and data protection practices.

3.1.3 Employees are expected to comply with information security requirements and support the protection of information assets through responsible workplace practices.

3.2 Workforce Responsibilities

3.2.1 Information security is a shared responsibility across the organization.

3.2.2 Employees, contractors, and authorized users are expected to follow applicable information security policies, standards, procedures, and guidelines.

3.2.3 Access to information systems and data shall be granted, used, and managed in accordance with business requirements and authorized permissions.

3.3 Third-Party Information Security

3.3.1 DMW extends its information security expectations to suppliers, service providers, consultants, and business partners that access or process company information.

3.3.2 Third parties shall be expected to protect information entrusted to them and comply with applicable contractual, legal, regulatory, and information security requirements.

3.3.3 Information security considerations may be incorporated into supplier selection, vendor management, and third-party engagement processes.

3.4 Information Security Assessments

3.4.1 DMW may conduct periodic reviews, assessments, audits, monitoring activities, vulnerability analyses, or other appropriate evaluations to identify information security risks and opportunities for improvement.

3.4.2 The Company may periodically evaluate information security controls and vulnerabilities to strengthen cybersecurity resilience and risk management practices.

4.0 GOVERNANCE AND ACCOUNTABILITY

4.1 Senior Management oversees the implementation of this policy and supports the effective management of information security risks.

MASTER COPY

VERSION NO. 1	MANUAL TITLE SUSTAINABILITY POLICIES	DOCUMENT NO. SUST-POL-002
	DOCUMENT NAME INFORMATION SECURITY POLICY	REVISION NO. 0
		EFFECTIVITY DATE SEPTEMBER 09, 2026
		PAGE NO. 4 OF 4

- 4.2 Relevant functions are responsible for implementing information security controls, monitoring risks, supporting compliance, and responding to information security incidents.
- 4.3 Employees are expected to support the information security commitments outlined in this policy as part of their day-to-day responsibilities.
- 4.4 Information security responsibilities may be assigned to relevant functions to support policy implementation and continual improvement.
- 4.5 Information security risks, incidents, vulnerabilities, and emerging threats are periodically reported through appropriate governance and management channels to support oversight, risk management, and continual improvement of information security practices.

5.0 GOVERNANCE AND REVIEW

5.1 Legal Compliance and Best Practice

DMW complies with applicable laws and regulations relating to information security, cybersecurity, data protection, and privacy, and seeks to adopt recognized industry best practices where appropriate.

DMW seeks to align its information security practices with recognized information security standards and frameworks, including ISO/IEC 27001 principles, where appropriate and feasible.

5.2 Monitoring and Continuous Improvement

Information security risks, controls, initiatives, and practices are periodically reviewed to support continual improvement.

5.3 Management Oversight

Senior Management oversees implementation of this policy and promotes responsible information security practices throughout the organization.

5.4 Periodic Review

This policy shall be reviewed annually and updated as necessary to reflect changes in business operations, technology, regulatory requirements, information security risks, and emerging best practices.

PREPARED BY:  Antoinette Marie M. Baltazar Asst. Sustainability Manager	APPROVED BY:  Delfin Angelo C. Wenceslao President and CEO	MASTER COPY	
---	--	--------------------	--

The use, disclosure, reproduction, modification, transfer of the document for any purpose in any form or by any means without the approval from D.M. Wenceslao & Associates, Incorporated (DMW) is strictly prohibited and may be subject to disciplinary and/or legal action.