	DCTV-POL-001 Information Security Policy Statement - Public

Document ID:	DCTV-POL-001	Effective Date:	11.16.2025
Version No.:	v1.0	Classification:	Public

Approval Signatures:

Name	Title	Signature	Approval Date
Richard D. Calleja	Chief Executive Officer	RDC	11.15.2025
Philippe Saubier	ISO Implementation & Certification Manager	PSA	11.11.2025
G. De La Pena	External ISO Consultant / Adviser	GDLP	11.11.2025

Document Control Footer:

Version	Effective Date	Details / Changes	Prepared By	Reviewed By	Approved By
1.0	Nov 12, 2025	Initial Document	Philippe Saubier – ISO Implementation & Certification Manager	Gindhel De la Pena, Lead Consultant	Richard D. Calleja – CEO

DCTV	**DCTV-POL-001 Information Security Policy Statement - Public**

Table of Contents

1. Purpose

The purpose of this Information Security Policy is to define DCTV management's direction and support for information security in alignment with business objectives and legal, regulatory, and contractual obligations. This policy provides the framework for the establishment and continual improvement of the Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022.

2. Scope

This policy applies to all personnel, information assets, systems, applications, cloud services, and physical facilities, including headquarters, branches, data centers, and authorized remote work environments, as defined in DCTV ISMS Scope Statement.

3. Information Security Objectives

DCTV is committed to ensuring confidentiality, integrity, and availability of information; protecting systems from unauthorized access; supporting business continuity; complying with legal requirements; and promoting security awareness.

4. Principles and Commitment

Top Management commits to leadership, a risk-based approach, continual improvement, training and awareness, and compliance with security standards and regulations.

This commitment is demonstrated by:

- Defining and approving the ISMS framework encompassing various information security-related policies and procedures, and comprehensive risk management.
- Establishing information security objectives that are aligned with the organization's strategic goals and with this documented information security policy statement.
- Ensuring allocation of adequate logical, physical, and technological resources for establishing, maintaining, and assessing an effective information security management system.
- Providing regular training and appropriate initiatives to enhance employees' awareness of information security.
- Ensuring all applicable laws, regulations, and contractual requirements related to information security are complied with and reviewed annually.
- Ensuring the periodic review and continuous improvement of the ISMS to adapt to new risks and evolving business needs.

5. Roles and Responsibilities

Top Management: Approves policy and ensures resources.
ISMS Manager: Oversees implementation and monitoring.
IT Manager: Implements technical controls.
Employees: Follow policies and report incidents.

6. Supporting Policies and References

Includes but not limited to: Acceptable Use Policy, Access Control Policy, Backup & Recovery Policy, Incident Management Policy, Cryptography Policy, Physical Security Policy, Supplier Security Policy.

7. Communication and Awareness

This policy will be communicated to all personnel, who must acknowledge their understanding.

This policy will be made available to all external interested parties by posting it on office walls, the company website, and social media platforms.

Training is required at onboarding and annually.

8. Review and Maintenance

This policy will be reviewed annually or upon changes to business, regulations, or security incidents. Updates require CEO approval.

9. Enforcement

Non-compliance may result in disciplinary action, termination, or legal consequences.