LOWEY DANNENBERG

Security Manual for Public Distribution

Version 1.0

Last Revised Date: December 30, 2019

TABLE OF CONTENTS

1.0 Information Security Policy

1.1 Purpose

The Partners of Lowey Dannenberg, P.C. (the "Firm") operate as a national law firm and is committed to preserving the confidentiality, integrity and availability of all the physical and electronic information assets throughout the Firm in order to preserve its competitive edge, profitability, legal, regulatory and contractual compliance. Information and information security requirements will continue to be aligned with Lowey Dannenberg's goals and the Information Security Management System (ISMS) is intended to be a mechanism for information sharing and for reducing information-related risks to acceptable levels.

1.2 Goals

The Firm is committed to safeguard the confidentiality, integrity and availability of all physical and electronic information assets of the organization and its customers to ensure that regulatory, operational and contractual requirements are fulfilled. The overall goals for information security are:

- Develop, implement and review policies and processes.
- Ensure compliance with current laws, regulations and guidelines.
- Identify and review all risks and impacts of breaches and develop objectives for risk reduction.
- Comply with requirements for confidentiality, integrity and availability for the Firm's stakeholders.
- Establish controls for protecting information and information systems against theft, abuse and other forms of harm and loss.
- Provide a safe and secure environment for clients' data.
- Ensure the availability and reliability of systems and services.
- Ensure confidentiality of data.
- Ensure that the Firm can continue their services even if an incident occurred.
- Work with employees to maintain the responsibility for, ownership of and knowledge of information security such that the risk of security incidents is reduced.
- Maintain communications with employees, customers, and interested parties.
- Continually improve the information security system.

The partners and all employees are committed to an effective Information Security Management System in accordance with its strategic business objectives.

1.3 Security Strategy

Lowey Dannenberg's current strategic business plan and risk management framework provide the context for identifying, assessing, evaluating and controlling information-related risks through the establishment and maintenance of an ISMS. The Risk Assessment, Statement of Applicability and Risk Treatment Plan identify how information-related risks are controlled. The senior partners are responsible for the management and maintenance of the risk treatment plan. Additional risk assessments may, where necessary, be carried out to determine appropriate controls for specific risks.

Business continuity and contingency plans, data backup procedures, avoidance of viruses and hackers, access control to systems and information security incident reporting are fundamental to this policy. Control objectives for each of these areas are contained in this and are supported by specific documented policies and procedures.

1.4 Security Objectives

Lowey Dannenberg aims to achieve specific, defined information security objectives, which are developed in accordance with the business objectives, the context of the organization, the results of risk assessments and the risk treatment plan.

All staff of the Firm are expected to comply with this policy and with the ISMS that implements this policy. All staff, and certain external parties, will receive appropriate training. The consequences of breaching the information security policy are set out in the Firm's disciplinary policy and in contracts and agreements with third parties.

The ISMS is subject to continuous, systematic review and improvement. The Firm has established management commitment to support the ISMS framework and to periodically review the security policy. This policy will be reviewed to respond to any changes in the risk assessment or risk treatment plan.

In this policy, "information security" is defined as preserving the availability, confidentiality, and integrity of physical and information assets. In this context:

- **Preserving** means that management, all full time or part time employees, sub-contractors, project consultants and any external parties have, and will be made aware of, their responsibilities (which are defined in their job descriptions or contracts) to preserve information security, to report security breaches (in line with the policy) and to act in accordance with the requirements of the ISMS. All Staff will receive information security awareness training and more specialized Staff will receive appropriately specialized information security training.

- **Availability** means that information and associated assets should be accessible to authorized users when required and therefore physically secure. The computer network must be resilient and Lowey Dannenberg must be able to detect and respond rapidly to incidents (such as viruses and other malware) that threaten the continued availability of assets, systems and information.

- **Confidentiality** means ensuring that information is only accessible to those authorized to access it and therefore to preventing both deliberate and accidental unauthorized access to the Firm's information, proprietary knowledge, and its systems.

- **Integrity** involves safeguarding the accuracy and completeness of information and processing methods, and therefore requires preventing deliberate or accidental, partial or complete, destruction or unauthorized modification, of either physical assets or electronic data. There must be appropriate contingency, data backup plans and security incident reporting. The Firm must comply with all relevant data-related legislation in those jurisdictions within which it operates.

- **Physical assets** include, but not limited to, computer hardware, data cabling, telephone systems, filing systems and physical data files.

- **Information assets** include information printed or written on paper, transmitted by post or shown in films, or spoken in conversation, as well as information stored electronically on servers, website(s), extranet(s), intranet(s), PCs, laptops, mobile phones and PDAs, as well as any removable media, backup tapes and any other digital or magnetic media, and information

transmitted electronically by any means. In this context, "data" also includes the sets of instructions that tell the system(s) how to manipulate information (i.e. the software: operating systems, applications, utilities, etc.). of the Firm.

1.5 Communications

Lowey Dannenberg and such partners that are part of our integrated network and have been made aware of our ISMS.

A security breach is any incident or activity that causes, or may cause, a break down in the availability, confidentiality or integrity of the physical or electronic information assets of Lowey Dannenberg will be communicated as deemed necessary.

This policy is communicated to all staff upon hire or significant change. This policy is reviewed for effectiveness and suitability on at least an annual basis or upon significant organizational change.

2.0 Document Revision History

DATE	VERSION	UPDATED BY	COMMENTS
10/1/2019	0.1	Steve Conley	Initial draft publication
12/30/2019	1.0	Steve Conley	Final version one