**Data Protection Policy**

Your privacy is important to Rosenthal & Rosenthal, Inc. Our information security program (“Data Protection Policy”) is effective as of February 2023 and explains the administrative, technical, and physical safeguards Rosenthal & Rosenthal, Inc. (“Rosenthal & Rosenthal” or “we”, “us” or “our”) has in place to protect the data that it collects, creates, uses, and maintains.

**Updates to this Data Protection Policy**

This Data Protection Policy is subject to change. We update this Data Protection Policy periodically as warranted. As a part of developing and implementing this Data Protection Policy, Rosenthal & Rosenthal will conduct and base its information security program on a periodic, documented risk assessment, whenever there is a material change in Rosenthal & Rosenthal’s business practices that may implicate the security, confidentiality, integrity, or availability of records containing information, or when circumstances so require. This Data Protection Policy has been developed in accordance with, *inter alia*, the requirements of the Gramm-Leach-Bliley Act Safeguards Rule, 16 C.F.R. §§ 314.1 to 314.6, the Massachusetts Data Security Regulation, 201 Code Mass. Regs. 17.01 to 17.05, and other similar US state laws, however, this should not be construed as a concession by Rosenthal & Rosenthal as to the applicability of any particular law or regulation to its operations, including with respect to the collection, protection and/or dissemination of data.

**Purpose of the Data Protection Policy**

The purpose of our Data Protection Policy is to enable Rosenthal & Rosenthal to the extent practicable, to:

1. Ensure the security, confidentiality, integrity, and availability of electronically stored information Rosenthal & Rosenthal collects, creates, uses, maintains and/or disseminates (“Data”);
2. Protect against anticipated threats or hazards to the security, confidentiality, integrity, or availability of Data;
3. Protect against unauthorized access to or use of Rosenthal & Rosenthal’s Data that could result in substantial harm or inconvenience to any customer or employee of Rosenthal & Rosenthal;
4. Define an information security program that is appropriate to Rosenthal & Rosenthal’s size, scope, and business, its available resources, and the amount of Data that Rosenthal & Rosenthal owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information;
5. Comply with data and information-related legal obligations; and
6. Follow best practices for Data governance and security.

**Kinds of Data We Protect**

We may collect Data in the course of your use of, or registration with, our website, mobile applications, and social sites, through your computer, smartphone, tablet or other mobile devices. For example, when you create an account or apply for a service, you may provide us with certain personal information. This type of personal information may include:

* **Contact information** such as name, telephone and mobile number(s), and email address with any required security code, access code, or password that would permit access to an individual’s personal, medical, insurance, or financial account.
* **Identifiers** such as Social Security number, driver’s license number, or other government-issued identification number including passport number, or tribal identification number.
* **Account information** such asaccount number or debit or credit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual’s financial account, or any personally identifiable financial information or consumer list, description, or other grouping derived from personally identifiable financial information.
* **Biometric data** such as an image of a fingerprint, retina, or iris, collected from the individual and used to authenticate the individual during a transaction.

Rosenthal & Rosenthal also take steps to protect sensitive Data including but not limited to, customer lists, business and client development plans, and documents created or exchanged in connection with any of the services we offer.

**How We Protect Your Data**

Rosenthal & Rosenthal has developed, implemented, and maintained administrative, technical, and physical safeguards to protect the security, confidentiality, integrity, and availability of Data that Rosenthal & Rosenthal owns or maintains on behalf of others.

***Administrative Safeguards***

Rosenthal’s administrative safeguards include:

1. A designated “Qualified Individual” who manages this Data Protection Policy;
2. Identification of internal and external risks and regular assessment of whether the existing safeguards adequately control identified risks;
3. Training for employees in security program practices and procedures with management oversight;
4. Selecting service providers that are capable of maintaining appropriate safeguards and requiring service providers to maintain safeguards by contract; and
5. Adjusting the Data Protection Policy in light of business changes or new circumstances.

***Technical Safeguards***

Rosenthal & Rosenthal’s technical safeguards includes maintenance of a security system covering its network (including wireless capabilities) and computers that, at a minimum, and to the extent technically feasible, supports:

1. Secure user authentication protocols, including:
   1. Controlling user identification and authentication with a reasonably secure method of assigning and selecting passwords (ensuring that passwords are kept in a location or format that does not compromise security) and by using other technologies, such as biometrics or token devices;
   2. Restricting access to active users and active user accounts only and preventing terminated employees or contractors from accessing systems or records; and
   3. Blocking a particular user identifier’s access after multiple unsuccessful attempts to gain access or placing limitations on access for the particular system.
2. Secure access control measures, including:
   1. Restricting access to records and files containing protected information to those with a need to know to perform their duties;
   2. Assigning to each individual with computer or network access unique identifiers and passwords (or other authentication means, but not vendor-supplied default passwords) that are reasonably designed to maintain security;
   3. Encryption of all protected information traveling wirelessly or across public networks;
   4. Encryption of all protected information stored on laptops or other portable or mobile devices, and to the extent technically feasible, protected information stored on any other device or media (data-at-rest);
   5. Logging of all attempts to read from or write to any file containing protected information, where such log shall include the date of the attempt, whether the attempt to read from or write to that file was successful, and to the extent technically feasible, the identity of the individual attempting to read from or write to that file;
   6. Reasonable system monitoring for preventing, detecting, and responding to unauthorized use of or access to protected information or other attacks or system failures;
   7. Reasonably current firewall protection and software patches for systems that contain (or may provide access to systems that contain) protected information; and
   8. Reasonably current system security software (or a version that can still be supported with reasonably current patches and malicious software (“malware”) definitions) that (1) includes malware protection with reasonably current patches and malware definitions, and (2) is configured to receive updates on a regular basis.

***Physical Safeguards***

Rosenthal’s physical safeguards include:

1. Physical security measures to protect areas where protected information may be accessed, including restricted physical access, and storing records containing protected information in locked facilities, areas, or containers;
2. Preventing, detecting, and responding to intrusions or unauthorized access to protected information, including during or after data collection, transportation, or disposal; and
3. Secure disposal or destruction of protected information, whether in paper or electronic form, when it is no longer to be retained in accordance with applicable laws or accepted standards.

***Additional Safeguards***

Rosenthal & Rosenthal’s safeguards also include:

1. Implementation and periodic review of technical and, as appropriate, physical access controls to:
   1. Authenticate and permit access to protected information only to authorized users; and
   2. Limit authorized users’ access only to protected information that they need to perform their duties and functions;
   3. Identifying and managing the data, personnel, devices, systems, and facilities that enable Rosenthal & Rosenthal to achieve its business purposes according to business priorities, objectives, and Rosenthal & Rosenthal’s risk management strategy;
   4. Encrypting protected information that Rosenthal & Rosenthal holds when it is at rest or in transit over external networks, unless Rosenthal & Rosenthal determines that applying encryption is currently infeasible for its circumstances and the Qualified Individual reviews and approves effective compensating controls under Rosenthal & Rosenthal’s exceptions process;
   5. Adopting secure development practices for the in-house developed applications and procedures for evaluating, assessing, or testing the security of externally developed applications that in either case Rosenthal & Rosenthal uses to transmit, access, or store protected information;
   6. Implementing multifactor authentication for individuals accessing protected information or systems that handle protected information unless the Qualified Individual reviews and approves the use of reasonably equivalent or more secure controls under Rosenthal & Rosenthal’s exceptions process;
   7. Developing, implementing, and maintaining procedures for securely disposing of protected information in any format, including:
      1. Disposing of customers’ protected information no later than two years after the last date Rosenthal & Rosenthal uses it for provisioning a product or service to the relevant customer unless it is necessary for business operations or other legitimate business purposes, retention is otherwise required by law, or targeted disposal is not reasonably feasible due to the way Rosenthal & Rosenthal maintains it; and
      2. Periodically reviewing data retention policies to minimize the unnecessary retention of protected information.
   8. Anticipating and evaluating risk from changes to the information system or network, including the evaluation of security risks introduced by modifications, removals, or additions to Rosenthal & Rosenthal’s systems and networks; and
   9. Implementing policies, procedures, and controls to monitor and log authorized users’ activities and detect unauthorized access to, use of, or tampering with protected information by them.

**Inquiries**

Inquiries about this Data Protection Policy may be directed to:

John Kinney, CTO

Rosenthal & Rosenthal, Inc.

1370 Broadway

New York, NY 10018

Phone: (212) 356-1774

E-mail: [JKinney@rosenthalinc.com](mailto:JKinney@rosenthalinc.com)