Revolution Capital, Inc.
Comprehensive Written Information Security Program (WISP)

I. OBJECTIVE

This program has been executed on behalf of **Revolution Capital, Inc.** for the purposes stated below. Our objective, in the development and implementation of this comprehensive written information security program ("WISP") is to create effective administrative, technical and physical safeguards for the protection of personal information of residents of the Commonwealth of Massachusetts and for our clients who reside elsewhere and to comply with obligations under 201 CMR 17.00. The WISP sets forth our procedure for evaluating our electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting personal information of those with whom we do business. For the purposes of this WISP "personal information" means a person's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such person: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a person's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information.

II. PURPOSE

The purpose of the WISP is to: (a) ensure the security and confidentiality of personal information; (b) protect against any anticipated threats or hazards to the security or integrity of such information; (c) protect against the unauthorized access to or use of such information in a manner that creates a substantial risk of identity theft or fraud.

III. SCOPE

In formulating and implementing the WISP we will: (a) identify reasonably foreseeable internal and external risks to security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (b) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (c) evaluate the sufficient of the existing policies, procedures, customer information systems, and other safeguards in place to control risks; (d) put safeguards in place to minimize those risks consistent with the requirements of 201 CMR 17.00; and (e) regularly monitor the effectiveness of those safeguards:

IV. DATA SECURITY COORDINATOR

We have designated Amy Witherbee to implement, supervise and maintain the WISP as the Data Security Coordinator ("DSC"). The DSC will be responsible for: (a) implementation of the WISP; (b) training employees, managers, owners and independent contractors who have access to personal information on elements of the WISP and certifying that all such persons have been made familiar with the firm's requirements for the protection of personal information; (c) regular testing of the WISP's safeguards; (d) requiring third party service providers by contract to implement and maintain appropriate security measures; (e) regular evaluations of the ability of each of our third party service providers to implement and maintain appropriate security measures for the personal information to which we have permitted them access, consistent with 201 CMR 17.00; and (f) reviewing the scope of the security measures in the WISP at least annually, or whenever there is a material change in our business practices that might impact the security or integrity of records containing personal information.

V. INTERNAL RISKS

To combat internal risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and to evaluating and respond, where necessary, to the

effectiveness of current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

1. A copy of the WISP must be distributed to each employee and contractor who might gain access to the personal information through firm records;
2. employees and contractors who are given access to personal information are required to conform to the provisions of the WISP and are prohibited from any nonconforming use of personal information during or after the employment and/or contract period;
3. the amount of personal information we collect shall be limited to that which is reasonably necessary to accomplish our legitimate business purposes, or necessary for compliance with other state or federal regulations;
4. physical and electronic access to records containing personal information shall be limited to those persons who are reasonably required to know such information in order to accomplish our legitimate business purpose or to enable us to comply with other state or federal regulations;
5. all security measures shall be reviewed at least annually, or whenever there is a material change in our business practices that may reasonably impact the security or integrity of records containing personal information. The DSC shall be responsible for this review and shall fully apprise management of the results of that review and any recommendations for improved security arising out of that review;
6. terminated employees or contractors must return all records containing personal information, in any form, that may at the time of such termination be in the former employee's possession;
7. a terminated employee's or contractor's physical and electronic access to personal information must be immediately blocked or terminated. The DSC shall maintain a secured master list of all lock combinations, passwords and keys;
8. any current employee's or contractor's user ID's and passwords must be changed periodically;
9. employees must report any suspicious or unauthorized use of customer information;
10. whenever there is an incident that requires notification under M.G.L. c.93H, sect.3, there shall be an immediate mandatory post-incident review of events and actions taken, if any, with a view to determining whether any changes in our security practices are necessary in order to improve the security of personal information for which we are responsible;
11. paper or electronic records containing personal information shall be disposed of only in a manner that complies with M.G.L. c.931;
12. all laptops or other devices used to access personal information shall be password-protected; all such devices shall require re-login when a computer has been inactive for more than a few minutes; and
13. employees who are found to have violated the processes and procedures herein shall be subject to disciplinary action. Disciplinary measures may include but are not limited to a probationary period of supervision for the employee, revocation of certain authorizations or termination as necessary to protect personal information.

VI. COMBATTING EXTERNAL RISKS

To combat external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information, and to evaluate and respond, where necessary, to the effectiveness of the current safeguards for limiting such risks, the following measures are mandatory and are effective immediately:

1. We maintain reasonable, current firewall protection and operating system security patches on all systems and devices processing personal information in keeping with industry standards;
2. all such security software or hardware are kept current, in accordance with industry standards, on any device or system processing personal information;
3. to the extent technically feasible, any personal information stored on laptops or other portable devices is encrypted, as is all records and files transmitted across public networks or wirelessly. "Encryption" shall mean the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key, unless further defined by regulation;

4. all computer systems are monitored for unauthorized use of or access to personal information;
5. there are secure user authentication protocols in place, including: (1) protocols for control of user IDs and other identifiers; (2) a reasonably secure method of assigning and selecting passwords, or use of unique identifier technologies; (3) control of data security passwords to ensure that such passwords are kept in a location.
6. client personal information is not maintained on laptops or other portable devices;
7. hard copy files containing client personal information are kept securely within the office and scanned as soon as possible to a digital format before being disposed of in a manner that complies with M.G.L. c.931;
8. electronic files containing client personal information are maintained on a cloud-based system for which data security safeguards have been evaluated and approved by the DSC.

The firm has designated Douglas Soons as Chief Compliance Officer.

The above policies and procedures shall next be reviewed on or before February, 2023.