The ID Register

Information Security Program

November 2019

The ID Register - Information Security Program

I. Policy Statement

The ID Register ("The ID Register") Written Information Security Program (the "Program") is a set of comprehensive guidelines and policies designed to safeguard all Personal Information maintained by The ID Register. It is intended to comply with applicable laws and regulations on the protection of Personal Information that is stored, accessed or collected at The ID Register or for The ID Register's operations.

II. Overview and Purpose

This Program complies with regulations issued by the Commonwealth of Massachusetts entitled "Standards For The Protection Of Personal Information Of Residents Of The Commonwealth" ("Massachusetts Standards") [201 Code Mass. Regs. 17.00]. This Program was adopted and implemented to comply with regulations issued under the information safeguards provisions of Title V of the Gramm-Leach-Bliley Act ("GL-B Act") [15 USC 6801(b) and 6805(b)(2)] and the applicable rules and regulations thereunder, specifically, the Securities and Exchange Commission's ("SEC") Regulation S-P "Safeguards Rule" ("Reg. S-P") [17 CMR 248.30]. The ID Register is not itself subject to the G-L-B Act or Reg. S-P.

Under U.S. law, The ID Register is required to adopt and implement written policies and procedures that are reasonably designed to safeguard Personal Information. The ID Register has implemented a number of policies to protect such information, and this Program should be read in conjunction with these policies, which are cross-referenced at the end of this document.

Under European Union Law, The ID Register is required to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

The purpose of this Program is to:

- Ensure the security and confidentiality of Personal Information in a manner fully consistent with industry standards;
- Ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- Provide a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing
- Establish a comprehensive information security program for The ID Register that contains policies that address administrative, technical and physical safeguards that are reasonably designed to safeguard Personal Information in compliance with European Union, Channel Islands and United States of America federal and state laws and regulations;
- Establish policies and procedures that are reasonably designed to protect against any anticipated threats or hazards to the security or integrity of Personal Information; *and*
- Establish policies and procedures that are reasonably designed to protect against unauthorized access to or use of Personal Information that may result in substantial harm or inconvenience to any person to whom that Personal Information relates.

III. Scope

This Program applies to any Personal Information stored, accessed or collected at The ID Register or for The ID Register's operations. It covers all Personal Information stored or accessed on computing systems, servers or networks, and electronic data owned, controlled by or in the custody of The ID Register. This Program also applies to Personal Information stored or accessed on applications owned or licensed by The ID Register, whether on premise or cloud-based.

This Program applies to all The ID Register employees and personnel, whether full- or part-time, including contract and temporary workers, hired consultants and interns, who are connected to The ID Register network or who have an account or any other form of access to information technology systems and applications owned or licensed by The ID Register. Certain aspects of this Program also extend to certain contracted third-party vendors (see section VII.D for further information) that receive Personal Information from or on behalf of The ID Register.

IV. Definitions

The ID Register - means The ID Register to the extent permitted by applicable local law, any affiliated companies to which it is associated by common ownership or control.

Personal Information - Personal Information means any information concerning an individual, including The ID Register employees and clients that, if improperly accessed or acquired, would create a risk of identity theft or fraud to the individual. For the purposes of this Program, Personal Information includes: (a) all nonpublic personal information as defined by the G-L-B Act and all applicable rules and regulations thereunder, including Reg. S-P, (b) "personal information" as it is defined under the Massachusetts Standards.

Examples of personal information as defined in the aforementioned Acts include, but are not limited to an individual's first and last name or first initial and last name, in combination with:

- Social Security number;
- Driver's license number or state-issued identification card number;
- Account number, credit card or debit card number, with or without any required security code, access code, personal identification number (PIN) or password, that would permit access to a person's account;
- Information a consumer provides to The ID Register on an application to obtain a financial product or service from The ID Register;
- Account balance information, payment history, overdraft history, and credit or debit card purchase information; *or*
- The fact that an individual is or has been The ID Register's customer or has obtained a service from The ID Register.

Personal Information as defined in the General Data Protection Regulation ("GDPR") is any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person being one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Information that relates to institutional investors who are not individual natural persons is not "Personal Information."

We intend to safeguard your Personal Information and to that end we implement physical, organizational and technical measures to help protect your Personal Information from unauthorised access, use or disclosure. Such measures include staff training and awareness and are reviewed regularly.

V. Development and Assessment of Risks

The ID Register has, on an ongoing basis, developed and implemented this Program in order to:

- Identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing Personal Information;
- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Personal Information;
- Evaluate the sufficiency of existing safeguards in place to control risks to Personal

Information;
- Put safeguards in place to minimize those risks; *and*
- Implement regular monitoring of the effectiveness of those safeguards and reporting thereon.

VI. Roles and Responsibilities

The ID Register's Director and, in his absence, the Management Team consisting of the Legal Manager, Project Manager and Operations Manager is responsible for implementing, supervising and maintaining this Program. The Director is specifically responsible for:

Implementing this Program;

- Overseeing regular testing of the effectiveness of the safeguards outlined in this Program;
- Ensuring that training of all employees regarding the security practices outlined in this Program will occur at the initial employee onboarding and on at least an annual basis thereafter;
- Evaluating the ability of any of The ID Register's potential and existing third party service providers and third party vendors to implement and maintain appropriate security measures to safeguard Personal Information to which they have been granted access,
- Verifying that such third party service providers are contractually obligated to implement and maintain appropriate security measures as it relates to the Personal Information they receive that is controlled by The ID Register;
- Overseeing the annual review of this Program and any necessary revisions to this Program;
- Actively engaging in the analysis and response to any incidents as addressed more fully in The ID Register's Incident Response Plan;
- Preparing annual information security reports for the Board of Directors of The ID Register;
- Engaging with senior management on issues relating to cybersecurity resources and cybersecurity risks;

and

- Creating additional IT security policies and supplementing this Program as needed.

In addition, all The ID Register employees and personnel are responsible for maintaining the confidentiality and integrity of Personal Information and must take reasonable steps to protect the data from unauthorized use, access, disclosure or alteration. All The ID Register employees and personnel are required to access, store and maintain records containing Personal Information in compliance with this Program. All The ID Register employees and personnel are required to report potential data incidents as outlined in The ID Register Incident Response Plan.

VII. Security

A. Governance and Risk Assessment

The ID Register's Director maintains an up-to-date organizational structure chart which indicates who is responsible for information security and cybersecurity matters and with which matters they engage.

The ID Register, via the Director will prepare annual information security reports for the Board of Directors of The ID Register and will engage with senior management on issues relating to cybersecurity resources and cybersecurity risks, including regulatory risks.

The ID Register will periodically evaluate its cybersecurity risks and, on at least an annual basis, will conduct a risk assessment and penetration test to identify cybersecurity threats, vulnerabilities and potential business and compliance consequences. The ID Register will take reasonable steps to retain records relating to such risk assessments and penetration testing as well as those records related to any remedial steps taken in response to identified threats and vulnerabilities.

B. Access Rights and Controls

Access

The ID Register takes reasonable steps to restrict access to records and files containing Personal Information to those employees who need Personal Information in order to perform their job duties. The ID Register has implemented access controls that are designed to prohibit access by employees who do not have a legitimate business need for such access. The ID Register:

- Restricts access to Personal Information to active users and active user accounts only.
- Prevents terminated employees and those employees with certain changes in status from accessing records containing Personal Information. A change in status may include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect an employee's access to The ID Register data.
- Retains records and documentation related to the tracking of employee access rights, changes to access rights and any approvals for those changes, as well as records related to a former employee's last date of employment and the date his/her access to The ID Register's system was terminated. The ID Register also takes reasonable steps to retain information related to (i) current employees who have been reassigned to a new group or function, including the date of the reassignment and the date on which access to The ID Register's systems was modified, if applicable; and (ii) instances in which system users received entitlements or access to firm data, systems or reports in contravention of firm policies or without required authorization, as well as any remediation efforts taken in response to such occurrences.
- Performs user access audits on a quarterly basis to review which employees have access to Personal Information.
- Blocks access to user accounts after multiple unsuccessful attempts to gain access.

Authentication and Authorization

The ID Register implements basic controls to prevent unauthorized access to systems or Personal Information. The ID Register controls access to Personal Information via the management of user credentials, authentication and authorization methods, including:

Parameter	**Policy Settling**
Minimum Length	8 Characters
Maximum Age	90 Days
Complexity requirements	• Uppercase alphabetic character • Lowercase alphabetic character • Numerical character • Cannot be derived from username

Periodic Internal Security Audits

The ID Register conducts periodic internal network security audits on all server and computer system logs to discover, to the extent reasonably feasible, possible unauthorized access to or disclosure, misuse, alteration, destruction or other compromise of Personal Information. The ID Register takes reasonable steps to retain information related to those internal audits.

C. Data Loss Prevention

The ID Register ensures robust controls for data loss prevention and takes the following steps to prevent the loss of Personal Information from its servers:

- Ensures control of data security passwords to ensure that passwords are kept in a location and/or format that does not compromise the security of the data they protect.
- Monitors for potentially unauthorized data transfers.
- Monitors the volume of content transferred outside of The ID Register by its employees or third parties, such as by email attachments or uploads.
- Implements policies with respect to where Personal Information should and should not be stored.
- Encrypts all transmitted records and files containing Personal Information.
- Ensures robust controls in the areas of patch management and system configuration.
- Ensures there is reasonably up-to-date firewall protection and that operating system security patches are reasonably designed to maintain the integrity of Personal Information.
- Maintains reasonably up-to-date versions of system security agent software which must include malware protection and reasonably up-to-date virus definitions that are set to receive the most current security updates on a regular basis.
- Takes appropriate steps to backup data in an effort to ensure backups are complete, up-to-date and disconnected from The ID Register's systems (either physically or via cloud-based storage).

The ID Register takes steps to maintain the physical security of Personal Information and IT systems. The ID Register:

- Maintains its IT systems in locations secured against theft and reasonably foreseeable damage.
- Secures access to its offices by key cards and maintains a log of key card activity.
- Does not allow its employees to transfer and store Personal Information on mobile devices; but only in accordance with the terms of The ID Register's Acceptable Use of Technology Policy and following the employees' completion and submission of the Usage Agreement.
- Instructs its employees not to maintain or keep hard copy documents containing Personal Information outside of The ID Register's premises, except as specifically authorized by the Director for legitimate business purposes and/or as stated in other policies and trainings.

D. Vendor Management

All The ID Register's infrastructure is hosted on the Microsoft Azure cloud pursuant to the security provisions found at http://www.theidregister.com The ID Register continuously reviews the security of the Microsoft cloud and is notified automatically of security and availability incidents.

With respect to third-party service providers and vendors, The ID Register:

- Conducts an appropriate level of due diligence on potential new vendors and takes reasonable steps to select and retain third-party service providers that are capable of

maintaining appropriate security measures to protect Personal Information consistent with the ways in which The ID Register protects Personal Information and in accordance with any applicable state and federal laws and regulations;

- Is taking steps to require its third-party vendors by contract to implement and maintain such appropriate security measures for Personal Information;

- Considers vendor relationships as part of its ongoing risk assessment process and will take reasonable steps to monitor such service providers by conducting an initial intake assessment, requiring an annual update regarding any significant change to the vendor's information security practices that could potentially have a security impact on The ID Register and/or The ID Register's data that contains Personal Information; *and*

- Takes reasonable steps to keep an up-to-date list of third-party vendors with access to the firm's network or data, as well as a description of the services those third-party vendors provide and the contractual terms related to their access of firm networks and data.

E. Training

A copy of this Program and the Incident Response Plan is made available to each current employee and every new employee at the beginning date of their employment. Training for all current employees will be held annually to detail their obligations under relevant provisions of this Program. New employees will be trained on their obligations under this Program within a reasonable period of time after their start date.

The Director will take reasonable steps to retain records of the training the firm provides to its employees regarding information security and risks. The records will describe the training methods employed, the date of the training, the topics included in the training and the groups of participating employees. Samples of written guidance or materials provided to employees in connection with the training will be retained to the extent practicable.

VIII. Appropriate Use and Enforcement

All The ID Register employees are instructed to advise the Director of any activities, operations or events which appear to pose risks to the security of Personal Information. If the Director is involved with these risks, employees are encouraged and invited to advise the Group Data Protection Officer of such risks. Employees who violate this Program may be subject to disciplinary action, up to and including termination. In appropriate cases, The ID Register may refer violations of this Program to law enforcement officials.

IX. Related Policies and Procedures

The following The ID Register policies provide guidance that relates to this Program:

- Incident Response Plan
- The ID Register's Acceptable Use of Technology Policy

X. Effective Date

This Written Information Security Program was implemented on 16 January 2017 and supersedes all prior policies.

The ID Register will review this Program at least annually and reserves the right to change, modify, or otherwise alter this Program at its sole discretion and at any time as it deems circumstances warrant.