Equation Research Data Breach Response Policy

1.0 Purpose

The purpose of the policy is to establish the goals and the vision for the breach response process. This policy will clearly define to whom it applies and under what circumstances, and it will include the definition of a breach, staff roles and responsibilities, standards and metrics (e.g., to enable prioritization of the incidents), as well as reporting, remediation, and feedback mechanisms. The policy shall be well publicized and made easily available to all personnel whose duties involve data privacy and security protection.

Equation Research, LLC Information Security's intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how Equation Research, LLC's established culture of openness, trust and integrity should respond to such activity. Equation Research, LLC is committed to protecting Equation Research, LLC's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

1.1 Background

This policy mandates that any individual who suspects that a theft, breach or exposure of Equation Research, LLC Protected data or Equation Research, LLC Sensitive data has occurred must immediately provide a description of what occurred via e-mail privacy@equationresearch.com or by calling 303-465-3803.
This e-mail address, phone number, and web page are monitored by the Equation Research, LLC's Information Security Administrator. This team will investigate all reported thefts, data breaches and exposures to confirm if a theft, breach or exposure has occurred. If a theft, breach or exposure has occurred, the Information Security Administrator will follow the appropriate procedure in place.

2.0 Scope

This policy applies to all whom collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of Equation Research, LLC research participants. Any agreements with vendors will contain language similar that protects research participants.

3.0 Policy Confirmed theft, data breach or exposure of Equation Research, LLC Protected data or Equation Research, LLC Sensitive data

As soon as a theft, data breach or exposure containing Equation Research, LLC Protected data or Equation Research, LLC Sensitive data is identified, the process of removing all access to that resource will begin.

The incident response team will handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- Finance (if applicable)
- Legal
- Communications
- Human Resources
- The affected unit or department that uses the involved system or output or whose data may have been breached or exposed
- Additional departments based on the data type involved, Additional individuals as deemed necessary by the Executive Director

Confirmed theft, breach or exposure of Equation Research, LLC data

The president will be notified of the theft, breach or exposure. IT, along with the designated team, will analyze the breach or exposure to determine the root cause.

Work with Forensic Investigators

As provided by Equation Research, LLC cyber insurance, the insurer will need to provide access to forensic investigators and experts that will determine how the breach or exposure occurred; the types of data involved; the number of internal/external individuals and/or organizations impacted; and analyze the breach or exposure to determine the root cause.

Equation Research, LLC’s response team will determine how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected.

4.0 Definitions

Encryption or encrypted data – The most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text;

Plain text – Unencrypted data.

Hacker – A slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s).

Protected Health Information (PHI) --- Under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

Personally Identifiable Information (PII) --- Any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered

Protected data --- See PII and PHI

Information Resource --- The data and information assets of an organization, department or unit.

Safeguards --- Countermeasures, controls put in place to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets. Safeguards help to reduce the risk of damage or loss by stopping, deterring, or slowing down an attack against an asset.

Sensitive data --- Data that is encrypted or in plain text and contains PII or PHI data. See PII and PHI above.

5.0 Revision History

Version	Date of Revision	Author	Description of Changes
1.0	September 17, 2018	Rachel Bell, GDPR Officer, Equation Research, LLC	Initial version