Consumer Breach Management Plan

Issued: December 10th, 2020

APPLIES TO: All Consumers

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.

AST's 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 AST's established culture of openness, trust and integrity should respond to such activity. AST's Information Security is committed to protecting AST's employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly.

POLICY:

BACKGROUND

This policy mandates that any individual who suspects that a theft, breach or exposure of AST's protected data or AST's sensitive data has occurred must immediately provide a description of what occurred via email to dataprivacy@astcorporation.com or by mail at AST LLC, 4343 Commerce Court #701, Lisle, IL 60532. This email address and mailbox are monitored by the AST 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.

SCOPE

This policy applies to all who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of AST's members. Any agreements with vendors will contain similar language that protects AST.

POLICY FOR CONFIRMED THEFT, DATA BREACH OR EXPOSURE OF AST'S PROTECTED DATA OR AST'S SENSITIVE DATA

As soon as a theft, data breach or exposure containing AST's protected data or AST's sensitive data is identified, the process of removing all access to that resource will begin.

The CEO will chair an incident response team to handle the breach or exposure.

The team will include members from:

- IT Infrastructure
- IT Applications
- Finance
- Legal
- Communications
- Client Services/Sales
- 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 CEO

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

DEVELOP A COMMUNICATION PLAN

The incident response team will work with AST's communications, legal and human resource departments to decide how to communicate the breach to: a) internal employees, b) the public, and c) those directly affected in a legally compliant manner.

OWNERSHIP AND RESPONSIBILITIES

- Sponsors are those members of the AST community that have primary responsibility for maintaining any particular information resource. Sponsors may be designated by any AST Executive in connection with their administrative responsibilities, or by the actual sponsorship, collection, development, or storage of information.
- Information Security Administrator is that member of the AST community, designated by the CEO or the CIO, who provides administrative support for the implementation, oversight and coordination of security procedures and systems with respect to specific information resources in consultation with the relevant Sponsors.
- Users include virtually all members of the AST community to the extent they have authorized access to information resources, and may include staff, trustees, contractors, consultants, interns, temporary employees and volunteers.
- The Incident Response Team shall be chaired by Executive Management and shall include, but will not be limited to, the following departments or their representatives: IT-Infrastructure, IT-Application Security; Communications; Legal; Management; Financial Services, Client Services and Sales; Human Resources.

ENFORCEMENT

Any AST personnel found in violation of this policy may be subject to disciplinary action, up to and including termination of employment. Any third party partner company found in violation may have their network connection terminated.

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.
- 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.

REVISION HISTORY

Version	Date of Revision	Author	Description of Changes
1.0	December 10, 2020	AST	Initial version
1.1	February 2022	AST	Annual Review
1.2	February 2023	AST	Annual Review
1.3	3/16/2024	AST	Annual Review