Go-Cort, Inc. Data Breach Response Policy

Last Update Status: Updated January 2021

1. Overview

This policy mandates that any individual who suspects that a theft, breach, or exposure of Go-Cort, Inc. (DBA Apptoto) protected or sensitive data has occurred must immediately provide a description of what occurred via e-mail to support@apptoto.com, by calling 888-318-3765, or through the use of the Support Center web page at http://www.apptoto.com/support. This e-mail address, phone number, and web page are monitored by the Go-Cort, Inc. security team. 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 security team will follow the appropriate procedure in place.

2. 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.

Go-Cort, Inc.'s intentions for publishing a Data Breach Response Policy are to focus significant attention on data security and data security breaches and how the company should respond to such activity. Go-Cort, Inc. is committed to protecting its customers, employees, partners, and the company itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

3. Scope

This policy applies to all employees who collect, access, maintain, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personally identifiable information or Protected Health Information (PHI) of Go-Cort, Inc. customers. Any agreements with vendors will contain language similar that protects the company.

4. Policy

4.1. Confirmed theft, data breach, or exposure of Go-Cort, Inc. Protected or Sensitive data response

4.1.1. As soon as a theft, data breach, or exposure containing Go-Cort, Inc. Protected data or Sensitive data is identified, the process of removing all access to that resource will begin.

4.1.2. The Head of Engineering and Product will chair an incident response team to handle the breach or exposure.

4.1.2.1. The team will include members from:

- IT Infrastructure
- IT Applications
- Finance (if applicable)

- Legal
- Communications
- Customer Success (if customer data is affected)
- 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

4.1.2.2. The designated response team will analyze the breach or exposure to determine the root cause.

4.1.3. As provided by Go-Cort, Inc. 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.

4.1.4. Work with Go-Cort, Inc. 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.

5. Definitions

5.1. 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.

5.2. 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.

5.3. 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

5.4. Protected data - See PII and PHI

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

6. Policy Compliance

6.1. Compliance Measurement

Go-Cort, Inc. will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback from employees.

6.2. Exceptions

Any exception to the policy must be approved by Go-Cort, Inc. in advance.

6.3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

7. Revision History

Date of Change	Responsible	Summary of Change
October 2016	Frank Cort	Adopted and customized to Go-Cort LLC (DBA Apptoto)
January 2021	Frank Cort	Customized to Go-Cort, Inc. (DBA Apptoto)