



Document Number	002
File Name	Data Breach Contingency Policy_Ecommerce_092019.1.docx

Data Breach Contingency Policy – E-Commerce Site

1. Overview

Ideal System Solutions, Inc. (IDEAL) utilizes the Internet to provide online shopping via a secure e-commerce site. In the course of conducting business functions via the e-commerce site, we store data within our systems. To provide a policy and process in the event of an information/data breach within our E-commerce system.

2. Purpose

To protect the sensitive data that belongs to our customers, we have implemented a number of processes. These processes include, but are not limited to, encrypting data and utilizing Secure Hypertext Transfer Protocol (HTTPS). The purpose of these guidelines is to provide best practices for securing customer data in the event of an information/data breach.

3. Scope

IDEAL's e-commerce site has security measures in place to protect against the loss, misuse or alteration of data under our control. All users are assigned unique user names and passwords that must be entered each time you log on. We also use advanced security methods based on dynamic data and encoded session identifications, and host the site in a secure environment that uses a firewall and other advanced technology to prevent interference or access from unauthorized users. When our Site is accessed, Secure Socket Layer (SSL) technology protects information using both server authentication and data encryption to help ensure that data is safe, secure, and available only to you. These safeguards help prevent unauthorized access, maintain data accuracy, and ensure the appropriate use of data.

4. Policy Guidelines

In the event that our processes fail to prevent the theft of sensitive data, we will undertake the following:

- Customers that may be impacted by any data theft will be notified.
- Notification that data has been compromised will be given to the customer within 24 hours of obtaining this knowledge.
- At the request of the customer, we will place on record the contact information for any impacted financial institution (i.e. credit card issuer) and notify said institution within the same time frame as given above.
- We will communicate to the customer whatever information may aid their efforts to prevent data theft from causing harm to their organization. This may include an estimate of the number of records, End-Users, or accounts involved.

- Following any event that involves compromised data, we will collect feedback from the impacted customers. This feedback will be used to adjust this process to better serve our customers in any future event.
- Report information breach to proper government authorities per our Ideal Security Plan. This guideline applies to employees, contractors, consultants, temporary and other workers at IDEAL including all personnel affiliated with third parties.

5. Policy Compliance

5.1 Compliance Measurement

The IDEAL Security Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, business tool reports, internal and external audits, and feedback to the policy owner.

5.2 Exceptions

Any exception to the policy must be approved by IDEAL Security Team in advance.

5.3 Non-Compliance

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

6. Related Standards, Policies and Processes

None.

7. Definitions and Terms

None.

8. Revision History

Date of Change	Version	Responsible	Summary of Change
9/14/19	001	IDEAL Policy Team	New E-Commerce specific policy