

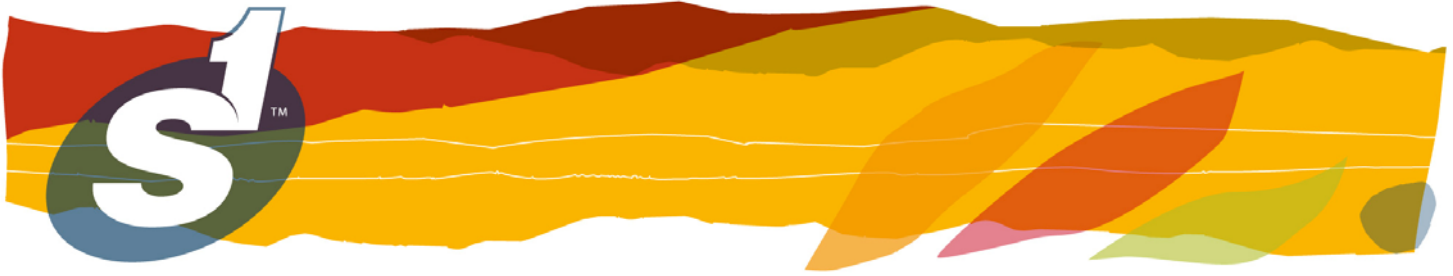
# Customer Information Privacy Policy

**S1 RISK AND INFORMATION SECURITY OFFICE**

S1 Risk and Information Security Office  
Customer Information Privacy Policy

Published: October 2008  
Revised: November 2010

S1 Corporation  
705 Westech Drive  
Norcross, Georgia 30092  
USA



**TABLE OF CONTENTS**

**1. CUSTOMER INFORMATION PRIVACY POLICY ..... 1**

1.1 S1 CUSTOMER INFORMATION PRIVACY STATEMENT ..... 1

1.2 DEFINITIONS ..... 2

1.3 COMPANY INTENTIONS AND MANAGEMENT RESPONSIBILITIES ..... 2

1.3.1 *Intentions and Objectives*..... 2

1.3.2 *Management Responsibilities*..... 2

1.3.3 *Data Classification Labels*..... 3

1.4 APPROPRIATE HANDLING OF PRIVATE INFORMATION..... 3

1.4.1 *Retention and Destruction of Private Information* ..... 3

1.4.2 *Removal of Private Information* ..... 3

1.4.3 *Preventing Disclosure* ..... 3

1.4.4 *Preventing Inadvertent Disclosure on Screens*..... 4

1.4.5 *Preventing Inadvertent Disclosure by Hardcopy* ..... 4

1.4.6 *Customer Notification of Disclosure*..... 4

1.5 PRIVATE INFORMATION ON COMPUTER AND COMMUNICATION SYSTEMS..... 4

1.5.1 *Encryption of Electronic Mail*..... 4

1.5.2 *Testing With Sanitized Data* ..... 5

1.6 PRIVATE INFORMATION AND END-USERS..... 5

1.6.1 *Consent for Collection Required*..... 5

1.6.2 *Change of Business Structure*..... 5

1.6.3 *Use of Outsourcing Organizations* ..... 5

1.7 REQUESTS FOR PRIVATE INFORMATION ..... 6

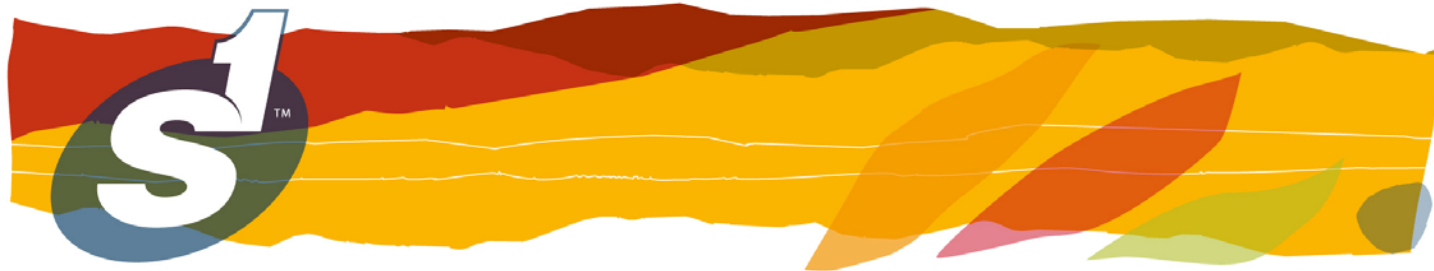
1.8 RESPONSIBILITIES ..... 6

1.8.1 *S1 Risk and Information Security Office*..... 6

1.8.2 *S1 Internal Audit* ..... 6

1.8.3 *S1 Risk and Information Security Committee (RISC)*..... 6

**APPENDIX A: DOCUMENT CHANGE CONTROL.....A**



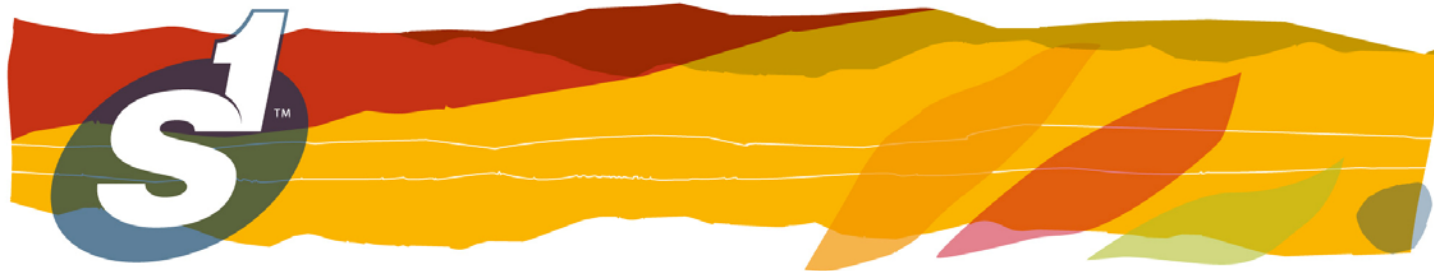
## 1. Customer Information Privacy Policy

### 1.1 S1 Customer Information Privacy Statement

The purpose of this policy is to provide our clients with a document illustrating the management and protection under which S1 Corporation ("S1") utilizes private information. We do not sell products or services directly to individual consumers, but instead is a Technology Services Provider (TSP or "Third Party Provider") to various financial institutions. As a normal part of these services, it is necessary for S1 to record, store, process, transmit, and otherwise handle personally identifiable information (hereafter referred to as "private information") about individual financial institution consumers ("consumers"). S1 has established appropriate controls to ensure that "Private Information" is disclosed only to those who have a legitimate business need for such access. S1 records, stores, processes, transmits, and handles "Private Information" as contractually directed by its financial institution customers ("customers"). S1 provides such "private information" to the customer who owns the information, the customer's consumers or an S1 affiliated third party (except as otherwise required by Federal, State, Local agencies, or applicable law).

S1 will make commercially reasonable efforts to comply with privacy provisions of all applicable laws and regulations including, but not limited to the GLBA and HIPAA. S1 is certified and complies with the U.S.-EU Safe Harbor Framework and the U.S.-Swiss Safe Harbor Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries and Switzerland.





## 1.2 Definitions

**Customer:** A financial institution that contracts with S1 to provide products and services.

**Consumer:** An individual who is a user of an S1 Customer's services.

**Affiliated Third Parties:** Individuals or organizations under contractual agreement with S1 to provide products and services as part of S1's business operations.

**Private Information:** Personally identifiable financial information that is provided by a consumer to a financial institution. This information may be obtained as a result of any transaction or any service with the consumer, or is otherwise obtained by the financial institution for some business purpose. It also includes any list, description, or other grouping of consumers (and publicly available information about them) that is derived using non-public private information.

## 1.3 Company Intentions and Management Responsibilities

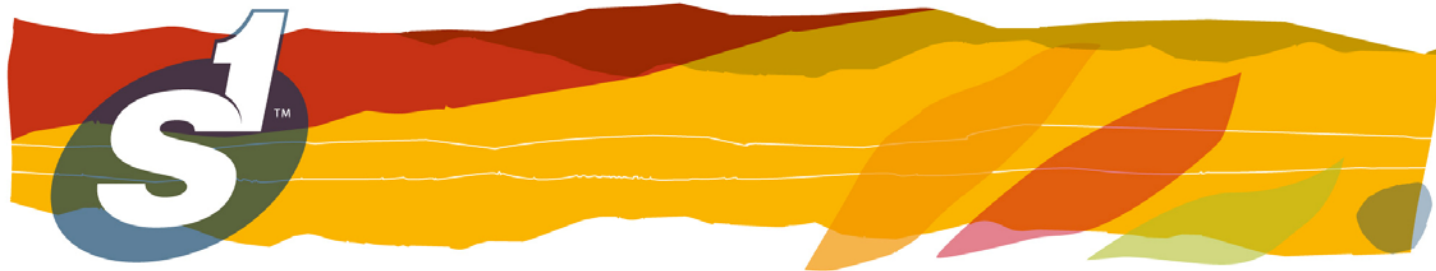
### 1.3.1 *Intentions and Objectives*

S1 ensures secure systems for the appropriate handling of Private Information. All such activities at S1 are intended to be consistent with both generally accepted privacy ethics and standard business practices.

### 1.3.2 *Management Responsibilities*

Management must make reasonable efforts so that all **Private Information** is used only as intended, and that precautions preventing misuse are both effective and appropriate. Management is responsible for establishing appropriate controls to ensure that **Private Information** is disclosed only to those who have a legitimate business need for such access.





### **1.3.3 Data Classification Labels**

Management must ensure that **Private Information** is consistently labeled to appropriately reflect its level of confidentiality.

## **1.4 Appropriate Handling of Private Information**

### **1.4.1 Retention and Destruction of Private Information**

Private Information is retained as contractually or legally required. When Private Information is no longer needed, it should be returned to the discloser, or destroyed by shredding, or by other destruction methods approved by S1's Risk and Information Security Office. Destruction of Private Information resident on computer disks and other magnetic media must be accomplished with an overwriting process. To assure the proper destruction of Private Information, disposal of computers with embedded hard disk drives or other data storage systems must proceed according to procedures issued by S1's Risk and Information Security Office.

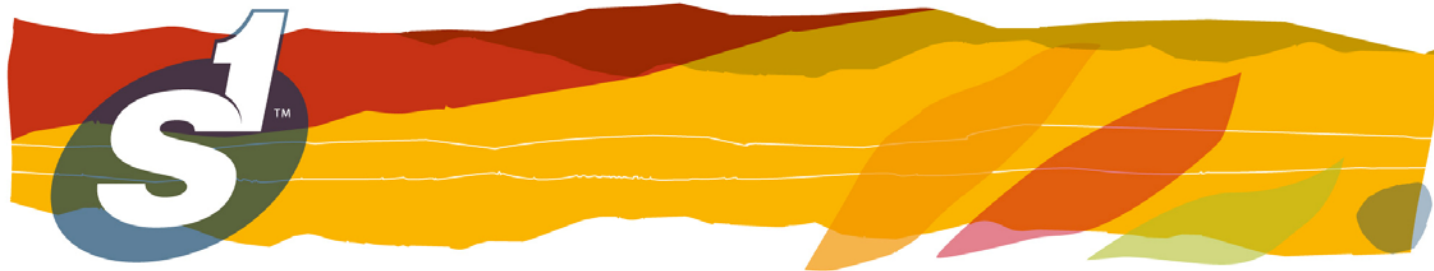
### **1.4.2 Removal of Private Information**

Every S1 employee is required to review and confirm understanding of the S1 Customer Information Privacy Policy. Private Information must not be removed from S1 offices or exported without appropriate authorization.

### **1.4.3 Preventing Disclosure**

Private Information is retained as contractually or legally required within a security zone. Physical and logical accesses to security zones are carefully controlled and only authorized personnel are given access to sensitive information. Systems that house Private Information are monitored to alert and notify of potential malicious activities.





#### ***1.4.4 Preventing Inadvertent Disclosure on Screens***

The display screens for all personal computers, workstations, and dumb terminals used to process Private Information must be positioned to reasonably minimize viewing through a window, by persons walking by a hallway, or by persons waiting in reception and related areas. All computers, workstations, and dumb terminals will be logged off, locked, or otherwise protected from unauthorized access or viewing while unattended.

#### ***1.4.5 Preventing Inadvertent Disclosure by Hardcopy***

Private Information in Hardcopy format should be conspicuously labeled to indicate the confidential nature of the document. If an S1 employee is handling Private Information and an unauthorized person enters the immediate area, then steps to conceal the information must promptly be taken. If the information is in physical form, the information can be covered with other material. If the information is displayed on a computer screen, the worker can invoke a screen saver or log off.

#### ***1.4.6 Customer Notification of Disclosure***

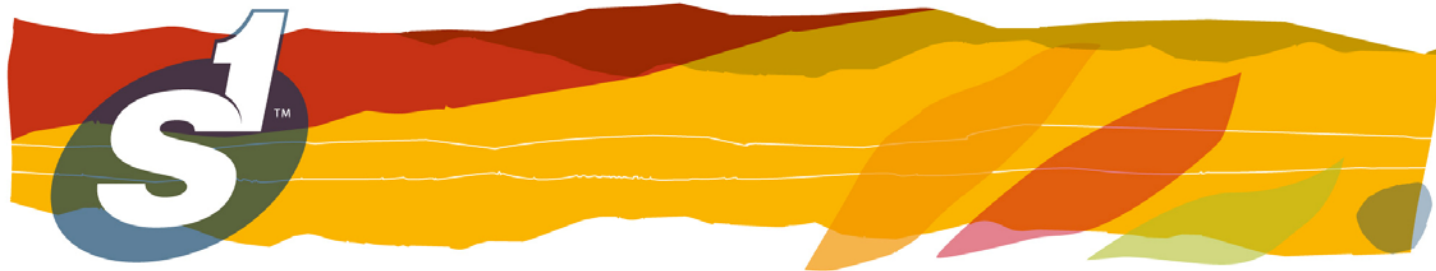
In accordance with applicable legal and regulatory requirements, S1 will respond to customers with any relevant malicious activities that are detected in an effort to prevent and mitigate fraud and identity theft.

### **1.5 Private Information on Computer and Communication Systems**

#### ***1.5.1 Encryption of Electronic Mail***

The only approved method for transmitting Private Information through electronic mail over a public network is via the use of S1 approved encryption technology.





### ***1.5.2 Testing With Sanitized Data***

All software testing for systems designed to handle Private Information must be conducted with “scrubbed” production data and/or manufactured test data. “Scrubbed” data consists of production data that has had its Private Information altered as to make it indecipherable from its original content. If an exception is required, and live data must be used, testing will be performed in a secured environment and data will be expunged appropriately when testing is completed. Permission for live data testing must be obtained in writing from S1’s Risk and Information Security Office.

## **1.6 Private Information and End-Users**

### ***1.6.1 Consent for Collection Required***

S1 does not collect Private Information about consumers. S1 does store Private Information obtained from its Customer’s system of record in order to make it available to consumers. This information has been previously collected by the Customers who are responsible for warranting that such information is obtained with the knowledge and consent of such End-Users.

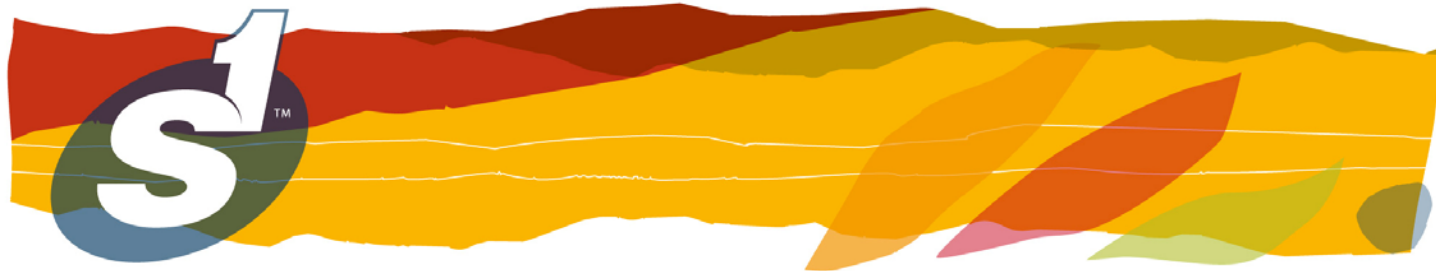
### ***1.6.2 Change of Business Structure***

Should S1 discontinue business operations, merge with or be acquired by another entity, or otherwise change the form of its organizational structure, S1 may, as part of the process for such event, need to share Private Information with another entity in order to continue to provide products and services.

### ***1.6.3 Use of Outsourcing Organizations***

S1 may outsource some or all of its information handling activities, and it may be necessary to provide Private Information to third parties to perform work under an outsourcing agreement.





In all such cases, the third parties involved must be bound to an obligation of confidentiality prohibiting them from further dissemination of this information and prohibiting them from using this information for unauthorized purposes.

### **1.7 Requests for Private Information**

All requests for Private Information that fall outside normal business procedures must be forwarded and approved by S1's General Counsel.

### **1.8 Responsibilities**

#### **1.8.1 *S1 Risk and Information Security Office***

The S1 Risk and Information Security Office is the department responsible for quarterly assessments to ensure compliance of Online and Archived Customer Information policies and procedures.

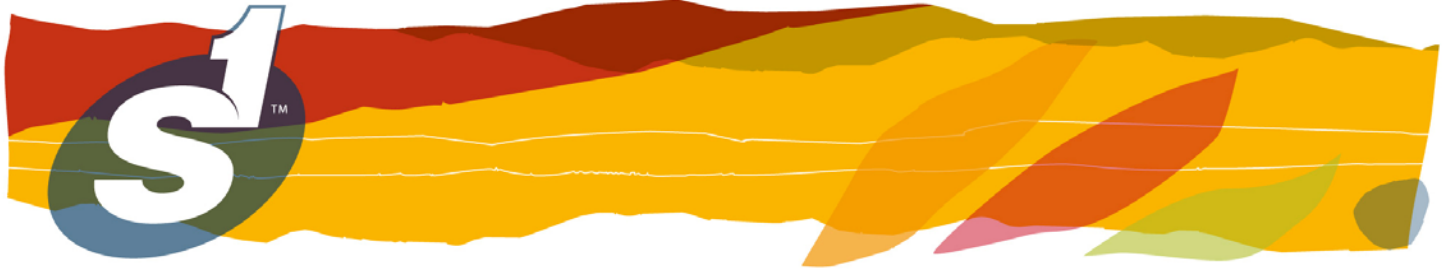
#### **1.8.2 *S1 Internal Audit***

The S1 Internal Audit is the department responsible for maintaining audit records that test compliance activities as designed by S1 policies.

#### **1.8.3 *S1 Risk and Information Security Committee (RISC)***

The S1 Risk and Information Security Committee (RISC) is the executive committee responsible for administration of S1 security and privacy policies.





## APPENDIX A: Document Change Control

This document is considered to be an S1 Office of Risk Management asset. Any changes made to this document must follow the appropriate version control procedures.

This section highlights the major changes to the document as it is revised.

Version Control			
Revision	Date	Author	Description
Version 1.3	October 2010	Thomas Hill	Annual Update
Version 1.2	October 2009	Thomas Hill	Annual Update
Version 1.1	October 2008	Thomas Hill	Red Flag Rule Inclusion
Version 1.0	August 2008	Thomas Hill	Annual Update

