Contents

1.0 Sheltered Harbor Overview ........................................................................................................4
   1.1 Sheltered Harbor Mission Statement ..................................................................................4
   1.2 Introduction .........................................................................................................................4
   1.3 Sheltered Harbor Background ...............................................................................................5
   1.4 Sheltered Harbor Objectives .................................................................................................5
   1.5 Sheltered Harbor Specifications Document .........................................................................6
   1.6 Ownership ............................................................................................................................7
   1.7 Governance and Participation ..............................................................................................7
   1.8 Terminology and Definitions ...............................................................................................8

2.0 Participant Eligibility & Enrollment ...........................................................................................9
   2.1 Sheltered Harbor Participant Eligibility ...............................................................................9
   2.2 Enrollment Process and Procedures ....................................................................................11
   2.3 Participation Dues ................................................................................................................12

3.0 Enrollment ..................................................................................................................................15
   3.1 Enrollment .............................................................................................................................15
   3.2 User Hardware and Software Requirements .......................................................................15
   3.3 Portal Access Credentials ....................................................................................................15
   3.4 Credential Revocation Procedures .....................................................................................15
   3.5 Unauthorized Use or Compromise of Credentials ...............................................................15
   3.6 Failed Access Credentials ..................................................................................................16
   3.7 Terminating Relationship ....................................................................................................16

4.0 Operations ..................................................................................................................................17
   4.1 Overview ...............................................................................................................................17
   4.2 Sheltered Harbor Operations ...............................................................................................17
   4.3 Sheltered Harbor Audit Verification & Certification Framework .........................................18

5.0 Traffic Light Protocol ..................................................................................................................20

6.0 Help Desk Policy and Procedures .............................................................................................21

7.0 Antitrust/Competition Provisions ..............................................................................................22
   7.1 Policy ....................................................................................................................................22
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.2</td>
<td>Vendor Discussion Policy</td>
<td>22</td>
</tr>
<tr>
<td>8.0</td>
<td>Code of Conduct for Officers and Directors</td>
<td>24</td>
</tr>
<tr>
<td>8.1</td>
<td>Code of Conduct</td>
<td>24</td>
</tr>
<tr>
<td>8.2</td>
<td>Obligations under the Code of Conduct</td>
<td>24</td>
</tr>
<tr>
<td>8.3</td>
<td>Code of Conduct Compliance</td>
<td>24</td>
</tr>
<tr>
<td>9.0</td>
<td>Confidentiality</td>
<td>26</td>
</tr>
<tr>
<td>9.1</td>
<td>Confidentiality Requirement</td>
<td>26</td>
</tr>
<tr>
<td>9.2</td>
<td>Confidentiality Agreement</td>
<td>27</td>
</tr>
<tr>
<td>10.0</td>
<td>Rules Modification and Precedence</td>
<td>28</td>
</tr>
<tr>
<td>10.1</td>
<td>Modification of Rules Approvals</td>
<td>28</td>
</tr>
</tbody>
</table>
1.0 Sheltered Harbor Overview

Sheltered Harbor was established as an organization to enhance the financial industry’s capabilities for securely storing and restoring account data during a disaster event by encouraging stakeholders to adopt and adhere to enhanced data security standards. With membership currently covering the majority of U.S. retail bank and brokerage accounts, Sheltered Harbor is a key step in the financial sector’s ongoing business continuity and resiliency efforts.

When activated, Sheltered Harbor will enable interoperability among firms and allow customers to access their account from another financial institution, should their “home” institution be unable to recover from a cyber-attack in a timely fashion. All consumer and account data stored as part of the Sheltered Harbor initiative is kept private—it is encrypted and protected from change.

1.1 Sheltered Harbor Mission Statement

Sheltered Harbor’s mission is to enhance capabilities for securely storing and restoring account data during a disaster event, encouraging all industry stakeholders to adopt and adhere to these standards, and certifying member compliance with the standards on a regular basis. Ultimately, the goal is to enable interoperability among firms.

1.2 Introduction

The threat of data security breaches against financial service providers is an increasing reality. As a result, the financial services industry bears a burden of responsibility to be extra vigilant in careful planning for recovery against such breaches. One proactive measure that can be taken to aid recovery is the safeguarding of critical data files on a regular basis in storage media and facilities that are inaccessible to any network. This concept has been shaped into an initiative led by Sheltered Harbor LLC (“Sheltered Harbor”), which seeks to define the methods necessary to implement a proactive defense.

The scope of Sheltered Harbor currently includes retail brokerage and deposit products. The information stored in accordance with Sheltered Harbor standards will be sufficient to establish account balances as of yesterday’s close of business, and to determine the individuals entitled to the funds in the account.
1.3 Sheltered Harbor Background

In recent years, cyber-attacks have been a persistent reality across all industries. Recent high profile cases show that the data an organization maintains is vulnerable to distortion or destruction by a cyber-attack; and by association, the services provided and ongoing operations that the organization conducts are susceptible to disruption (which may threaten the ongoing viability of the organization).

The financial industry is a target of cyber-attacks that could potentially breach data security measures and destroy a financial institution’s operating systems. The financial services markets are highly interconnected and this is a shared concern of all market participants. It is generally accepted that a catastrophic event such as a cyber-attack that renders one market participant inoperable could negatively impact many participants within the market. An example of this exists where the inoperable firm would not be able to fulfill its obligations to the market due to its impaired abilities. Given a severe enough attack, indirect impacts to the market may also exist, such as creating fear in retail customers of unaffected institutions who witness the fallout of a cyber-attack. This could cause disruption to the entire financial market.

The whole financial industry bears a burden of responsibility to be extra vigilant in planning for recovery against such breaches. One proactive measure that can be taken to aid recovery is the safeguarding of critical data files on a regular basis in storage media and facilities that are inaccessible to retrieval from any network.

This “air-gapped data-vault” concept shaped the Sheltered Harbor initiative, which seeks to define the methods necessary to implement a proactive defense. The scope of Sheltered Harbor is to protect the member firms’ data across both retail banking and retail brokerage products.

1.4 Sheltered Harbor Objectives

Sheltered Harbor is an industry driven initiative that recognizes the interconnectedness of all parties within the industry. The initiative looks to industry experts to define a set of standards that all Sheltered Harbor participants (“Participants”) will conform to in order to protect their firms’ data.

The Sheltered Harbor initiative focuses on three primary objectives:

1) Standards: Sheltered Harbor has established common File Formats and Standards for securely storing and recovering critical client account data.
2) Adoption: Sheltered will have enabled widespread adoption of its secure data protection standards.
3) Adherence: Sheltered Harbor will facilitate Member adherence to standards on at least an annual basis.
### Exhibit 1: The Sheltered Harbor Solution Overview

1. **Standards**
   - Establish a commonly agreed to data format and procedures for securely storing and restoring critical financial account information for U.S. banks and securities firms to enable restoration

2. **Adoption**
   - Encourage all industry stakeholders, including banks, brokerage firms, and service providers to adopt and adhere to Sheltered Harbor standards
   - Active participation from industry associations and regulators is key to rate of adoption

3. **Certification**
   - Certify member compliance with the established Sheltered Harbor standards on at least an annual basis, using accepted protocols
   - Sheltered Harbor will facilitate restoration simulations and participate in industry exercises

---

#### 1.5 Sheltered Harbor Specifications Document

The Sheltered Harbor Specifications document is the culmination of the work of multiple industry working groups tasked with defining a set of standards that all Sheltered Harbor Participants will conform to in order to protect their customers’ account data.

Sheltered Harbor describes Participant implementation of the standards for securely storing and recovering client account data, as well as Participant adherence requirements in the Sheltered Harbor Specifications document. This document is only available to Sheltered Harbor Participants. Sheltered Harbor maintains and updates the standards in the Specifications document through ongoing oversight and adaptation in response to developments in the industry.
Exhibit 2: Sheltered Harbor Specifications Summary

### End-of-Day File Production and Storage

**Issuing Financial Institution**
- Extract data; build data files based on SH file formats

**Data Vault**
- Provide file integrity check; compress and encrypt account data

- Transmit data to vault; validate integrity of data; secure data

- Banking file format is to be based on FDIC Part 360 format
- Brokerage file format is to be based largely on standard industry and vendor file formats including DTCC bulk transfer
- Sheltered Harbor extensions were developed to ensure fit for purpose (e.g. File Naming standard ensures unique identification of originating institution, as well context of each file’s origin)
- Data reasonability checks to compare control totals to other relevant metrics and to historical indications
- AES encryption algorithm is to be used for encryption
- Encryption key, initialization vector, tags are to be stored on immutable and non-volatile media
- Transmission data channel to require mutual authentication and to cryptographically secure contents
- File integrity is to be validated via comparison of the cryptographic hash value generated prior to sending data to vault and one generated by the vault
- A notification is to be sent to Sheltered Harbor after successful process completion

### Adherence

**Governance**
- Sheltered Harbor is responsible for governance and oversight of its ecosystem, including:
  - Admitting and accrediting members
  - Setting and updating standards
  - Enforcing the certification / accreditation process
  - Processing automated notifications of process completion

**Control Adherence Framework**
- Control environment principles
- Controls over file production design and implementation processes
- Controls over daily file production and storage processes

**Audit Verification & Certification Framework**
- Initial (“Pre-certification”) process
- Recurring annual audit certification
- Attestation report from internal or external audit
- Remediation for a failed audit

## 1.6 Ownership

Sheltered Harbor is wholly owned by FS-ISAC Inc. but maintains an independent Board of Directors ("Board") responsible for the strategy and governance.

FS-ISAC Inc. is a system of information exchange among entities in the financial services sector for the purposes of providing members with timely, accurate, and actionable warnings of physical, operational, and cyber threats or attacks on the financial services infrastructure or individual firms, and for collecting and providing information on potential vulnerabilities in the financial services infrastructure. More information on FS-ISAC Inc. may be found on www.fsisac.com.

## 1.7 Governance and Participation

Sheltered Harbor is an industry driven initiative that was created in response to a perceived threat to the financial system as a whole. As an industry driven initiative, its Board of Directors comprises a broad cross-section of representatives from its membership. Likewise, its executive team has been brought together from experienced industry professionals with a broad set of
expertise to establish the mission of Sheltered Harbor and set the standards governing security, technology and data management.

Sheltered Harbor will be governed and managed under the processes and authorities established by its Limited Liability Company Agreement. Its independent Board is composed of representatives from the membership and elects a Chairman or Co-Chairmen. The Board will meet regularly to review and discuss matters pertaining to the company, to provide oversight over company matters, and to provide strategic direction to the management team. Daily management of the company is the responsibility of the Chief Executive Officer, who coordinates Sheltered Harbor activities and is assisted by the core team and is advised by expert advisors.

Participation in Sheltered Harbor is open to all financial services firms, service providers, industry utilities and industry associations.

1.8 Terminology and Definitions

1. **Primary Contact** is defined as the person in the Participant firm to whom all Sheltered Harbor notices, invoices, and other information is delivered. The Primary Contact represents the Participant and attests to the Sheltered Harbor Board that its employees, agents and consultants who engage with Sheltered Harbor will comply with the Operating Rules and ensure strict confidentiality of Sheltered Harbor information. The Primary Contact is responsible for ensuring all Access Coordinators are current and have the need for credentials and have the appropriate authority to use the credentials issued by Sheltered Harbor.

2. **Access Coordinators** are those employees, agents and contractors identified by the Primary Contact as authorized to have Sheltered Harbor credentials.

3. **Member Proprietary Information** means any information in any form voluntarily provided by the Participant to Sheltered Harbor under these Operating Rules. Sheltered Harbor will handle the information in accordance with these Operating Rules.

4. **Sheltered Harbor Proprietary Information** means (i) any information in any form provided by Sheltered Harbor to Participants under these Operating Rules; and, (ii) any intellectual property defined and identified as such.

5. **Operator Proprietary Information** means all specifications, computer programs, upgrades, processes, know-how, and other intellectual property embedded in Sheltered Harbor, except as defined and documented as belonging to Sheltered Harbor.

6. **Sheltered Harbor Portal** or **Portal** refers to any internet site that provides access to the private information that is exclusively available to Sheltered Harbor Participants after successful completion of the authentication process.
2.0 Participant Eligibility & Enrollment

2.1 Sheltered Harbor Participant Eligibility

2.1(a) Participants in Sheltered Harbor will be limited to:

1. Banking or securities firms that offer Federal Deposit Insurance Corporation or Securities Investor Protection Corporation insured accounts, or credit unions that offer National Credit Union Share Insurance Fund insured accounts (the “Firm Participation Criteria”) are eligible to become Participants and shall be deemed to be “Firm Participants”.

2. Service providers that maintain payment, account or securities records on behalf of banking and securities firms are eligible to become Participants and shall be deemed to be “Industry Service Participants”.

3. Banking or securities industry associations are eligible to become Participants and shall be deemed to be “Association Participants”.

The Board of Directors and FS-ISAC may determine from time to time other criteria to allow entities to become eligible Participants.

The Board of Sheltered Harbor, at its discretion, can deny membership to any applicant.

It is the intent of Sheltered Harbor, consistent with its mission as set forth in Section 1.1 and subject to this Section 3.1(a), that any Person that meets the Firm Participation Criteria that desires to execute a Sheltered Harbor Participation Agreement (“Participation Agreement”) shall be eligible to become a Firm Participant, unless Sheltered Harbor, in consultation with FS-ISAC, determines in good faith that permitting such Person to become a Participant would reasonably be expected to result in a violation of Applicable Law by Sheltered Harbor, would reasonably be expected to result in liability to Sheltered Harbor or FS-ISAC or would reasonably be expected to create any franchise or reputational risk to Sheltered Harbor or FS-ISAC.

2.1(b) Other Requirements:

1. Participants must:
   i. Be able to provide evidence of their good standing with all appropriate regulatory bodies or trade groups recognized by Sheltered Harbor or FS-ISAC.
   ii. Adhere to all applicable regulations and laws, including antitrust, privacy, and other relevant laws;
   iii. Adhere to strict standards for professional conduct;
   iv. Remain current with all financial obligations to Sheltered Harbor;
2. International applicants for membership must have their regulated status by their host country vetted and verified by the Sheltered Harbor staff.

3. Participants are required to inform Sheltered Harbor within ten (10) Business Days if they cease to satisfy the eligibility criteria in Section 3.1(a). If a Participant ceases to satisfy the eligibility criteria, then such failure shall constitute a Participation Termination Event for such Participant as provided for in Section 3.1(c).

4. Sheltered Harbor may conduct periodic member eligibility reviews to assure compliance.

2.1(c) Participant Termination:

1. A Participant shall cease to be a Participant at the election of Sheltered Harbor upon the occurrence of any one of the following events (each a “Participation Termination Event”):
   i. the continuing failure by a Participant to pay any Participation Dues within thirty (30) days after receiving written notification from Sheltered Harbor of such failure;
   ii. any liquidation, dissolution or winding-up of the affairs of a Participant;
   iii. the merger, combination or Transfer of the Participant, or the Transfer of a substantial part of the Participant’s business, to another entity (other than to another Participant or to an entity that meets the eligibility criteria of Section 3.1(a) and Section 3.1(b));
   iv. the continuing failure by a Participant to satisfy the eligibility criteria in Section 3.1(a) and Section 3.1(b) within thirty (30) days after receiving written notification from Sheltered Harbor of such failure; or
   v. the Board of Directors of Sheltered Harbor, in consultation with FS-ISAC, determines in good faith that the continued subscription of a Participant would reasonably be expected to result in a violation of Applicable Law by Sheltered Harbor, would reasonably be expected to result in liability to Sheltered Harbor or FS-ISAC or would reasonably be expected to create any franchise or reputational risk to Sheltered Harbor or FS-ISAC.

2. A Participant may terminate its subscription as a Participant at any time upon written notice by such Participant to Sheltered Harbor.

Upon the termination of a Participant’s subscription, the terminated Participant shall have no further liability to Sheltered Harbor with respect to any unpaid Participation Dues; provided that, if a termination of a Participant’s subscription has occurred pursuant to Section 3.1(c)(2), the terminated Participant shall remain liable to Sheltered Harbor with respect to any Participation Dues required to be paid by such terminating Participant that were due more than 30 days prior to the date such terminating Participant delivers its termination notice pursuant to Section 3.1(c)(2).
Participant Revocation: Sheltered Harbor reserves the right to revoke participation in Sheltered Harbor if the Participants are found not to be compliant with the eligibility criteria, the Participation Agreement, timely payment of dues, or these Operating Rules.

Participant’s license to use Sheltered Harbor information will terminate upon termination of its subscription.

2.2 Enrollment Process and Procedures

2.2(a) Participants will enroll by completing the appropriate Participation Application, accepting the Participation Agreement and paying the applicable Participation Dues when invoiced. Participants will also identify the Primary Contact and authorized access coordinators within their organization (“Access coordinators”). Participant organizations and their users of Sheltered Harbor agree to abide by the Participation Agreement and the Operating Rules.

2.2(b) An organization wishing to become a Participant in Sheltered Harbor may obtain all relevant information including these Operating Rules and the Participation Agreement by contacting either its participating service provider or by contacting Sheltered Harbor directly at membership@shelteredharbor.org.

2.2(c) A signed Participation Agreement (which incorporates acceptance of these Operating Rules) and payment of Participation Dues as specified in the Participation Agreement constitute an application for enrollment. A signed Participation Agreement must be sent to Sheltered Harbor as directed below.

The address for delivery of paper and electronic applications is:
Sheltered Harbor Membership Operations
2020 Sunrise Valley Drive
Suite 230
Reston, Virginia 20191
membership@shelteredharbor.org

2.2(d) Sheltered Harbor will use trusted third party sources to verify applicant eligibility based on the information provided in Addendum 1 of the Participation Agreement. The Primary Contact and Access Coordinator(s) identification must be completed.

2.2(e) Upon receipt of a signed Participation Agreement, completion of the eligibility verification, and a determination by Sheltered Harbor in consultation with FS-ISAC that the Participant should be granted participation, Sheltered Harbor will invoice Participant for the Participation Dues as specified in the Participation Agreement. After payment of Participation Dues, participation will be enabled and a notification will be sent.
2.3 Participation Dues

2.3(a) Sheltered Harbor is a not-for-profit industry effort and, as such, only seeks to cover its operating costs. Sheltered Harbor intends to charge its Participants annual Participation Dues for (1) access to full set of specifications on how to ensure secure storage and recovery of their account data\(^1\), and (2) opportunity to receive a Sheltered Harbor certification\(^2\) once Participants implement a storage process compliant with these specifications.

2.3(b) Sheltered Harbor will charge Participation Dues to:

(i) Firm Participants based on the type of institution and the size of the institution, as defined by:
   1. Number of US depository accounts and US banking assets ($) for Participants that are banking firms
   2. Client assets and number of clearing clients for Participants that are securities firms

(ii) Association Participants and Industry Service Participants as determined in good faith by the Board of Directors

(iii) Participants which are Global Systemically Important Banks as defined by the Financial Stability Board are assessed a flat fee of $50,000

In its sole discretion, Sheltered Harbor Board of Directors reserves the right to adjust the metrics or the criteria which determines Participation Dues as it deems appropriate. Exhibit 3 outlines the structure for Participation Dues as of publication date.

\(^1\) Described in detail in the Sheltered Harbor Specifications document available to Participants

\(^2\) Described in detail in the Sheltered Harbor Specifications document available to Participants
Exhibit 3: Participation Dues Structure Overview

<table>
<thead>
<tr>
<th>Category</th>
<th>Fees</th>
</tr>
</thead>
<tbody>
<tr>
<td>G-SIBs</td>
<td>$50,000</td>
</tr>
<tr>
<td>Banks (1)</td>
<td>$250 - $25K, based on both US banking assets and US deposit accounts</td>
</tr>
<tr>
<td>Brokers (2)</td>
<td>$2.5K - $25K, based on both client assets and # of clearing clients</td>
</tr>
<tr>
<td>Service Providers</td>
<td>$5,000 (typically). Contact Sheltered Harbor for details</td>
</tr>
<tr>
<td>Associations</td>
<td>$2,500</td>
</tr>
</tbody>
</table>

1 See Exhibit 4 for detail
2 See Exhibit 5 for detail

For banks, Participant fees are determined based on both Participants’ Total US Banking Assets and Participant’s Total US Deposit Accounts to more accurately reflect bank size. Exhibit 4 below describes the exact fees applying at each level of Participant’s assets and accounts.

Exhibit 4: Annual Fee Assessment Schedule for Banks

<table>
<thead>
<tr>
<th>Assets</th>
<th>Accounts</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>&lt;$100mm</td>
<td>&lt;10K</td>
</tr>
<tr>
<td>2</td>
<td>&lt;$1Bn</td>
<td>&lt;500K</td>
</tr>
<tr>
<td>3</td>
<td>$1Bn - $50Bn</td>
<td>&lt;500K</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt;500K</td>
</tr>
<tr>
<td>4</td>
<td>&gt;$50Bn</td>
<td>&lt;1mm</td>
</tr>
<tr>
<td></td>
<td></td>
<td>&gt;1mm</td>
</tr>
</tbody>
</table>

For securities firms, Participant fees are determined based on both Client Assets3 and the Number of Clearing Clients. Exhibit 5 below describes the exact fees applying at each level of Participant’s client assets and clearing clients.

3 Including discretionary and non-discretionary assets
Exhibit 5: Annual Fee Assessment Schedule for Securities Firms

<table>
<thead>
<tr>
<th>Client Assets</th>
<th>Clearing Clients</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;$100mm</td>
<td>1 (self-clearer)</td>
<td>$2,500</td>
</tr>
<tr>
<td>&lt;50</td>
<td></td>
<td>$5,000</td>
</tr>
<tr>
<td>50 - 100</td>
<td></td>
<td>$10,000</td>
</tr>
<tr>
<td>&lt;$10Bn</td>
<td></td>
<td>$10,000</td>
</tr>
<tr>
<td>50 - 100</td>
<td></td>
<td>$25,000</td>
</tr>
<tr>
<td>&gt;$200Bn</td>
<td>or</td>
<td>$25,000</td>
</tr>
</tbody>
</table>

Participants with both banking and brokerage operations pay only a single fee based on the larger of the banking or the brokerage fee calculation (except for G-SIBs which are assessed a flat fee of $50,000)

2.3(c) Sheltered Harbor will notify each Participant of the applicable Participation Dues and provide for the invoicing and collection of such Participation Dues, which may be paid directly to Sheltered Harbor or via a Participant’s FS-ISAC account. Each Participant shall deposit its Participation Dues in cash, by wire transfer of immediately available funds, to the designated account of Sheltered Harbor or FS-ISAC set forth in the Participation Dues notice within thirty (30) days of receiving a Participation Dues notice.
3.0 Enrollment

3.1 Enrollment

Sheltered Harbor coordinator will contact the Primary Contact to activate the account once the application has been approved. Via the Sheltered Harbor Portal, the Primary Contact will receive access to Sheltered Harbor documentation and any other relevant materials available to Participants only.

3.2 User Hardware and Software Requirements

There are no special hardware or software requirements to use the Sheltered Harbor Portal. A participant must have the capability to access the Internet using commonly supported browsers.

3.3 Portal Access Credentials

3.3(a) Access credentials to the Sheltered Harbor Portal are issued to the members’ Access Coordinators. These are not anonymous. They will be allocated to individuals as determined by the participant and are tracked and monitored for use. It is the responsibility of the participants’ Primary Contact to manage and maintain internal control and the current status of these credentials.

3.3(b) Processes are established to initially set authentication credentials, reset authenticators, and reissue and invalidate authenticators when requested to by the Primary Contact or when suspicious access is attempted.

3.4 Credential Revocation Procedures

3.4(a) The Primary Contact may request replacement credentials from Sheltered Harbor at help@shelteredharbor.org.

3.4(b) If a credential is rejected on three separate occasions it will be disabled without notice to the Primary Contact. It is the responsibility of the Primary Contact to ensure Sheltered Harbor has current contact information for each Access Coordinator.

3.5 Unauthorized Use or Compromise of Credentials
ANY SUSPECTED COMPROMISE OR UNAUTHORIZED USE OF ANY CREDENTIAL MUST BE IMMEDIATELY REPORTED TO SHELTERED HARBOR AT HELP@SHELTEREDHARBOR.ORG.

3.6 Failed Access Credentials

If any credentials become inoperative, Sheltered Harbor must be contacted at content@shelteredharbor.org for instructions on how to receive a replacement and procedures for the return of the failed access credential(s) to Sheltered Harbor.

3.7 Terminating Relationship

Upon termination of the Participation Agreement for any reason, access credentials to the Sheltered Harbor portal will be terminated.
4.0 Operations

4.1 Overview

4.1(a) The Sheltered Harbor services and general overview of the operations follows. Sheltered Harbor Specifications document available to Participants has further detail on Sheltered Harbor roles and responsibilities.

1. The intent of Sheltered Harbor is to:
   - Improve resiliency of the US financial system by preventing loss of critical customer account data
   - Establish and maintain commonly agreed to data formats and procedures for securely storing and restoring critical financial account information for U.S. banks and securities firms to enable restoration
   - Promote and certify the use of common data formats and procedures for securely storing and restoring critical financial account information
   - When and if necessary, assist in facilitating the recovery of critical customer account data using the Sheltered Harbor procedures and playbooks

4.1(b) Via the Sheltered Harbor portal, Participants have access to Sheltered Harbor Specifications: a regularly updated document detailing how to fully and completely implement the Sheltered Harbor solution within an organization. Participants requiring assistance with implementation can contact help@shelteredharbor.org

4.1(c) In accordance with the terms of the Participation Agreement, Sheltered Harbor grants to Participant a license to use the Sheltered Harbor Specifications in a manner consistent with Participation Agreement and the Rules. Participant’s license to use Sheltered Harbor information will terminate upon termination of Participant’s membership.

4.2 Sheltered Harbor Operations

The Sheltered Harbor organization will maintain a core operating capability to support the ongoing development and support of the Sheltered Harbor initiative. Although much of the work to support its intent is done by participating organizations, several common operating functions will be addressed by this core. Examples of such functions include:

- Standards Development
- Membership Support & Communications
- Certification Management
4.3 Sheltered Harbor Audit Verification & Certification Framework

4.3(a) Along with the implementation of Sheltered Harbor procedures, all Participants are expected to attest and certify that the required controls and standards over Sheltered Harbor file production and storage processes, as well as restoration processes for those flies, are operating in accordance with criteria / standards established by Sheltered Harbor. The accreditation / certification process is evidenced by participating firm’s submission of the prescribed Sheltered Harbor Adherence Certification Reports.

Sheltered Harbor has chosen to utilize industry accepted audit standards / control frameworks in evidencing Participant adherence to Shelter Harbor specifications.

Sheltered Harbor will allow a Participant’s Internal Audit Department to provide a Sheltered Harbor Adherence Certification Report in lieu of external audit. The expectation is that the scope of work performed by Internal Audit would be the substantially the same as that performed by an external audit firm, that the work would be performed in accordance with audit standards defined by the Institute of Internal Auditors (IIA), and that the report would be addressed to a senior officer of the Participant institution and provided to Sheltered Harbor.

The required testing program and format of the Sheltered Harbor Adherence Certification Report will be continually updated to incorporate all Sheltered Harbor Specifications approved by its Board.

4.3(b) The following section outlines the requirements for meeting the Adherence Certification. A detailed description of the requirements is included in the Sheltered Harbor Specifications document.

1. Sheltered Harbor ‘Ready’ Self-Attestation Requirements and Reporting – requires an attestation that Participant has operationalized the Sheltered Harbor file production and storage processes in accordance with Sheltered Harbor specifications. Participants are encouraged to implement the Sheltered Harbor Specification as soon as practical for their organization, optimally within nine months of becoming a Participant. This attestation, in accordance with the Sheltered Harbor Specification, should be delivered to Sheltered Harbor within 90 days from the as of date.
Operating Rules

2. Sheltered Harbor “Set” Audit Requirements and Reporting - requires Participant to submit formal attestation, in accordance with the Sheltered Harbor Specification, certifying that the operationalized processes and controls over daily end-of-day file generation and storage adhere to Sheltered Harbor specifications. The Sheltered Harbor ‘Set’ report should be as of six months from the as of date of Sheltered Harbor “Ready” report and submitted within 90 days from the as of date.

3. Sheltered Harbor “Go” Audit Requirements and Reporting - requires Participants to submit an attestation, as defined in the Specification, certifying (1) that the operationalized processes and controls over daily end-of-day file generation and storage adhere to Sheltered Harbor specifications, as well as (2) the ability to restore account data by an external process in accordance with Sheltered Harbor specifications. The Sheltered Harbor “Go” report should be as of six months from the as of date of Sheltered Harbor “Set” report and submitted within 90 days from the as of date.

4.3(c) Participants will not be eligible to use the Sheltered Harbor designations, including but not limited to “Sheltered Harbor Ready”, “Sheltered Harbor Set”, “Sheltered Harbor Go” to describe their implementation status, internal controls, and data security protocols until they successfully complete the required certification process as described in the Sheltered Harbor Specifications document. Sheltered Harbor, in its sole discretion, reserves the right to permit Participants to use and to continue to use the Sheltered Harbor designations noted above upon successful completion of initial and follow-up certification. For avoidance of doubt, neither execution of this Agreement, nor payment of Participation Dues are alone sufficient to obtain the Sheltered Harbor designations.
5.0 Traffic Light Protocol

5.0(a) All information submitted, processed, stored, archived, or disposed of will be classified and handled in accordance with its classification.

5.0(b) Information will be classified using the Traffic Light Protocol (TLP), defined as:

<table>
<thead>
<tr>
<th>Color</th>
<th>When should it be used?</th>
<th>How may it be shared?</th>
</tr>
</thead>
<tbody>
<tr>
<td>RED</td>
<td>Use TLP RED when the information’s audience must be tightly controlled, because misuse of the information could lead to impacts on a party’s privacy, reputation, or operations. Target audience to which distribution is restricted must be specified.</td>
<td>Recipients may not share TLP RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.</td>
</tr>
<tr>
<td>AMBER</td>
<td>Use TLP AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</td>
<td>Recipients may only share TLP AMBER information with staff in their own organization who need to know, or with service providers to mitigate risks to the member’s organization if the providers are contractually obligated to protect the confidentiality of the information. TLP AMBER information can be shared with those parties specified above only as widely as necessary to act on the information.</td>
</tr>
<tr>
<td>GREEN</td>
<td>Use TLP GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community.</td>
<td>Recipients may share TLP GREEN information with peers, trusted government and critical infrastructure partner organizations, and service providers with whom they have a contractual relationship, who have a need-to-know but not via publicly accessible channels.</td>
</tr>
<tr>
<td>WHITE</td>
<td>Use TLP WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</td>
<td>TLP WHITE information may be distributed without restriction, subject to copyright controls.</td>
</tr>
</tbody>
</table>

5.0(c) If no marking is specified, the information shall be treated as Sheltered Harbor Confidential Information (TLP: Amber).

5.0(d) Information classified as Green, Yellow, or Red must be disclosed, transported, stored, transmitted, and disposed of in a safe and secure manner using controls appropriate to the level of classification. These controls include, but are not limited to, encryption, shredding, securely erasing, and degaussing of media.
6.0 Help Desk Policy and Procedures

Participants may contact Sheltered Harbor via email for Help Desk activities at membership@shelteredharbor.org.
Operating Rules

7.0 Antitrust/Competition Provisions

7.1 Policy

7.1(a) Sheltered Harbor, FS-ISAC, Inc., their Board of Directors, and their Members and Participants will comply with all laws and regulations governing antitrust and anticompetitive practices. Sheltered Harbor or FS-ISAC officers, directors, staff, and members must not engage in any conduct that may constitute violation of these laws, including but not limited to price fixing, group boycotts, or allocations of markets among organizations or institutions.

7.1(b) To assure compliance with this policy:

1. Sheltered Harbor Participants are prohibited from discussing any company-specific, competitively sensitive information, including terms, sales, conditions, pricing, or future plans, related to their firms or other firms, including vendors or service providers they engage;
2. Any Sheltered Harbor portals or forums are not to serve as a conduit for discussions or negotiations between or among vendors, manufacturers or security service providers with respect to any Participant or group of Participants;
3. Neither Sheltered Harbor or FS-ISAC Inc. staff, officers, and directors nor its Members, Participants, committees, and committee chairs are to recommend in any Sheltered Harbor-sponsored or FS-ISAC-sponsored exchange or forum in favor of or against the coordinated boycott or adoption of any company or product or service of particular manufacturers or vendors;
4. Each Sheltered Harbor Participant will determine the effect of the exchanged information on its individual purchasing and related decisions;
5. Any breach of these guidelines will be reviewed by the Boards of Directors of the FS-ISAC and Sheltered Harbor and may result in termination of the organization’s FS-ISAC and Sheltered Harbor memberships and forfeiture of remaining annual membership fees.
6. Committee chairs, directors or staff will designate a responsible party to publish and disseminate minutes of Board committee and association meetings.

7.2 Vendor Discussion Policy

Sharing of positive or negative views concerning products, services, or vendors is permitted. However, such sharing must be professional and courteous. The vendor community is vital to the mission of the association, as well as often being a direct and valuable supporter of Sheltered Harbor.
While information should flow freely, those sharing such views should be mindful of appropriate etiquette and focus on providing factual information. Tone and the sheer number of comments should be taken into account.
8.0 Code of Conduct for Officers and Directors

8.1 Code of Conduct

A Code of Conduct will apply to Sheltered Harbor directors and officers to provide guidance to help them recognize and deal with ethical issues; provide mechanisms to report unethical conduct; and to help foster a culture of honesty and accountability.

8.2 Obligations under the Code of Conduct

8.2(a) Directors and officers are responsible for the stewardship of Sheltered Harbor, assuring that it continues to have the critical capabilities needed to achieve its objectives.

8.2(b) Directors and officers have fiduciary duties to Sheltered Harbor, including the duties of care, obedience, and loyalty, and are obligated as a matter of corporate law to act in good faith to promote the best interests of Sheltered Harbor, including undivided loyalty to Sheltered Harbor. Directors and officers under this Code are obligated to:

1. Act honestly, in good faith and in the best interests of Sheltered Harbor, including but not limited to furthering the Sheltered Harbor mission and activities above those of other companies or organizations;
2. Follow guidelines established by the Board regarding how it will govern and conduct itself;
3. Refrain from speaking as an individual on behalf of the Board unless authorized to do so;
4. Appropriately avoid actual or apparent conflicts of interest.

8.2(c) Directors and officers are obligated to treat as confidential discussions at Board or committee meetings, including expressions of opinion and discussions. Board and committee decisions should be kept confidential until publicly disclosed by Sheltered Harbor. Confidentiality extends to, but is not limited to, all disclosures of trade secrets, proprietary know-how, financial information or other confidential information made to any director of officer.

8.3 Code of Conduct Compliance

8.3(a) The Chair of the Board should immediately be notified of any legal process from third parties calling for disclosure of any information received by a director in his or her role as a director or committee member.

8.3(b) Directors and officers must communicate any suspected violations of the Code promptly to the Chair of the Board. Suspected violations will be investigated by the Board or by a person or persons designated by the Board, and appropriate action will be taken in the event of any violations of this Code.
9.0 Confidentiality

9.1 Confidentiality Requirement

9.1(a) Directors, officers, staff and members may have access to or receive from Sheltered Harbor or the FS-ISAC, its members, or affiliated partners certain trade secrets and other information pertaining to the disclosing party or its employees, customers and suppliers.

9.1(b) Confidential information may be disclosed at member meetings, committee meetings, and meetings held by various working groups of Sheltered Harbor that may be constituted.

9.1(c) Directors, officers, staff and members agree that all such Confidential information obtained shall be considered confidential and proprietary to the disclosing party.

9.1(d) All information shared in Sheltered Harbor portals and forums is classified as Confidential (Amber) by default unless specifically classified otherwise.

9.1(e) Staff and contractors are required to execute a confidentiality agreement as a condition of employment. Participants, including directors and officers, are bound by the terms of the Participation Agreement.

9.1(f) Parties in possession of Confidential Information may be requested to disclose Confidential Information to law enforcement, a government authority or other third party, pursuant to subpoena or other legal order. To the extent allowed by law, the disclosing party will use reasonable and customary efforts to provide Sheltered Harbor with advance notice of such disclosure to allow Sheltered Harbor and impacted parties to seek an appropriate protective order or other relief to prohibit or limit such disclosure.

---

4 Recipients may only share AMBER information with staff in their own organization who need to know, or with service providers to mitigate risks to the member’s organization if the providers are contractually obligated to protect the confidentiality of the information. AMBER information can be shared with those parties specified above only as widely as necessary to act on the information.
9.2 Confidentiality Agreement

Recipients of Confidential Information will be obligated to:

1. Protect and preserve the confidential and proprietary nature of all Confidential Information;

2. Not disclose, give, sell or otherwise transfer or make available, directly or indirectly, any Confidential Information to any third party for any purpose, except as expressly permitted in writing by Sheltered Harbor and the disclosing party;

3. Not use, or make any records or copies of, the Confidential Information, except as needed in order to provide specific services in the conduct of their duties, or as required by law or regulations, or as needed to use the information effectively to mitigate risk in their respective organizations;

4. Limit the dissemination of the Confidential Information to those with the need to know the Confidential Information, provided that such individuals are obligated to maintain the confidential and proprietary nature of the Confidential Information;

5. Return all Confidential Information and any copies thereof as soon as it is no longer needed or immediately upon the disclosing party’s request, to the extent permitted by law and regulatory retention requirements;

6. Notify Sheltered Harbor immediately of any loss or misplacement of Confidential Information, and

7. Comply with any reasonable security procedures designated in the Confidentiality Agreement as may be prescribed by Sheltered Harbor for protection of the Confidential Information.
10.0  Rules Modification and Precedence

10.1  Modification of Rules Approvals

From time to time these Operating Rules and the Participation Agreement may be modified with the approval of the Board of Directors of Sheltered Harbor. E-mail notifications to current Participants will be provided at that time. All changes will be highlighted and/or annotated for applicability.